



DATA BREACH REPORTS

2016 End of Year Report



The ITRC Data Breach Report, and supplemental documents, are brought to you by CyberScout, formerly IDT911. We would like to thank CyberScout for their continued financial support.

CONTENTS

Information & Background on ITRC	2
Methodology	3
ITRC Breach Stats Report Summary	4
ITRC Breach Stats Report	5
ITRC Breach Report	45

The ITRC Data
Breach Report is
sponsored by:



Formerly  IDT911

CyberScout delivers a comprehensive suite of breach mitigation and identity management solutions to empower you to:

- Reduce your risk of a data breach occurring
- React swiftly and appropriately in the event a breach happens
- Manage the reputation of your organization and of those affected by the breach

Visit www.CyberScout.com or call **888.682.5911** today to learn more.

Identity Theft Resource Center would like to thank **CyberScout** for their continued financial support.

Information and Background on ITRC

Information management is critically important to all of us - as employees and consumers. For that reason, the Identity Theft Resource Center has been tracking security breaches since 2005, looking for patterns, new trends and any information that may better help us to educate consumers and businesses on the need for understanding the value of protecting personal identifying information.

What is a breach? The ITRC defines a data breach as an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure. This exposure can occur either electronically or in paper format. The ITRC will also capture breaches that do not, by the nature of the incident, trigger data breach notification laws. Generally, these breaches consist of the exposure of user names, emails and passwords without involving sensitive personal identifying information. These breach incidents will be included by name but **without** the total number of records exposed.

There are currently two ITRC breach reports which are updated and posted on-line on a weekly basis. The *ITRC Breach Report* presents detailed information about data exposure events along with running totals for a specific year. Breaches are broken down into five categories, as follows: business, banking/credit/financial, educational, Government/Military and medical/healthcare. The *ITRC Breach Stats Report* provides a summary of this information by category. Other more detailed reports may be generated on a quarterly basis or as dictated by trends.

It should be noted that data breaches are not all alike. Security breaches can be broken down into a number of additional sub-categories by what happened and what information (data) was exposed. What they all have in common is they usually contain personal identifying information (PII) in a format easily read by thieves, in other words, not encrypted.

The ITRC currently tracks seven categories of data loss methods: Insider Theft, Hacking/Skimming/Phishing, Data on the Move, Subcontractor/Third Party/BA, Employee error/Negligence/Improper disposal/Lost, Accidental web/Internet Exposure and Physical Theft. In some cases, there may be more than one category checked. For example, in the case of employee error which occurred with the Subcontractor.

The ITRC breach list also tracks four types of information compromised:

- Social Security number
- Credit/Debit Card number
- Email/Password/User Name
- Protected Health Information (PHI)
- Other/Undefined Type of Records

Methodology

The ITRC breach list is a compilation of data breaches confirmed by various media sources or notification lists from state governmental agencies. This list is updated daily, and published each Tuesday.

Breaches on this list typically have exposed information which could potentially lead to identity theft, including Social Security numbers, financial account information, or medical information. ITRC follows U.S. Federal guidelines about what combination of personal information comprise a unique individual, and the exposure of which will constitute a data breach.

Records Reported:

This field has been changed to more accurately reflect the circumstances surrounding the number of records exposed. The numeral "0" has been replaced with "Unknown" - recognizing the number of records may have been reported to some other entity (i.e. government or law enforcement), but is not provided in the information available to the ITRC.

Breach categories:

Business: This category encompasses retail services, hospitality and tourism, professional, trade, transportation, utilities, payment processors and other entities not included in the other four sectors. It also includes nonprofit organizations, industry associations, non-government social service providers, as well as life insurance companies and insurance brokers (non-medical).

Educational: Any public or private educational facility, from pre-school through university level. This category does not include scholarship providers, after school entities, or tutoring organizations.

Medical/Healthcare: Any medical covered entity (CE) or business associate (BA), as defined by HIPAA, in the healthcare industry. Also includes healthcare facilities and organizations which may be attached to schools and universities, and *may* include pharmaceutical manufacturers. Insurance companies may vary by industry – medical and long term insurance providers will be classified as medical healthcare. (Included on hhs.gov list).

Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Government/Military: Any city, county, state, national or military entity; or a department within one of these entities. In the event that a medical facility is also a government or military entity, it will be listed under Government/Military. Entities such as Veteran Association Medical Centers (VAMC) will be included in this sector.

Banking/Credit/Financial: This sector includes entities such as banks, credit unions, credit card companies, mortgage and loan brokers, financial services, investment firms and trust companies, payday lenders and pension funds (401 savings plans)

Identity Theft Resource Center

2016 Data Breach Category Summary

How is this report produced? What are the rules? See below for details.

Report Date: 1/18/2017

Totals for Category: Banking/Credit/Financial	# of Breaches: 52	# of Records: 72,262
	% of Breaches: 4.8%	%of Records: 0.2%
Totals for Category: Business	# of Breaches: 495	# of Records: 5,669,711
	% of Breaches: 45.3	%of Records: 15.5%
Totals for Category: Educational	# of Breaches: 98	# of Records: 1,048,342
	% of Breaches: 9.0%	%of Records: 2.9%
Totals for Category: Government/Military	# of Breaches: 72	# of Records: 13,869,571
	% of Breaches: 6.6%	%of Records: 37.9%
Totals for Category: Medical/Healthcare	# of Breaches: 376	# of Records: 15,942,053
	% of Breaches: 34.4	%of Records: 43.6%
Totals for All Categories:	# of Breaches: 1093	# of Records: 36,601,939
	% of Breaches: 100.0	%of Records: 100.0%

2016 Breaches Identified by the ITRC as of: 1/18/2017

Total Breaches: 1,093
Records Exposed: 36,601,939

The ITRC Breach database is updated on a daily basis, and published to our website on each Tuesday. Unless noted otherwise, each report includes breaches that occurred in the year of the report name (such as "2016 Breach List"), or became public in the report name year, but were not public in the previous year. Each item must be previously published by a credible source, such as Attorney General's website, TV, radio, press, etc. The item will not be included at all if ITRC is not certain that the source is real and credible. We include in each item a link or source of the article, and the information presented by that article. Many times, we have attributions from a multitude of media sources and media outlets. ITRC sticks to the facts as reported, and does not add or subtract from the previously published information. When the number of exposed records is not reported, we note that fact. Note: For data breach incidents involving only emails, user names, and/or passwords, the number of records are not included in the overall total number of records.

The ITRC Breach Report presents individual information about data exposure events and running totals for the year. The ITRC Breach Stats Report develops some statistics based upon the type of entity involved in the data exposure.

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Category: Banking/Credit/Financial

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20161231-30	Northern State Bank	WI	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161229-11	WestPark Capital	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161222-06	Federal Savings Bank	IL	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161222-01	Dover Federal Credit Union	DE	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161220-03	Bank of America	NC	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161220-02	Contact Solutions	VA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161219-04	Ameriprise	MN	Banking/Credit/Financial	Yes - Published #	350
ITRC20161216-16	SkyOne Federal Credit Union	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161216-13	Mann Mortgage, Inc.	MT	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161212-01	Anchor Loans	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161129-08	State Street Corporation	MA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161128-19	Capital One	VA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161128-18	Boeing Employees Credit Union	WA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161128-09	Ameriprise Financial	MN	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161128-07	Primerica	GA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161115-02	Baxter Credit Union	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161028-02	37th Parallel Properties Investment Group, LLC	VA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161027-02	Rocky Mountain Credit Union	MT	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161024-14	Clear One Funding, LP / WWC Capital Group, LLC	VA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161018-10	One Nevada Credit Union	NV	Banking/Credit/Financial	Yes - Published #	1,000
ITRC20161018-09	Broadview Mortgage	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161014-12	HSBC Securities USA, Inc.	NY	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161014-04	Santander	MA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161014-01	TD Bank / Santander	MA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161013-24	TD Bank	NJ	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20161013-22	HD Vest Investment Services	TX	Banking/Credit/Financial	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160923-14	Freddie Mac	VA	Banking/Credit/Financial	Yes - Published #	2,361
ITRC20160923-06	Premier America Credit Union	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160920-09	QR Lending	FL	Banking/Credit/Financial	Yes - Published #	1,487
ITRC20160919-15	Signature Financial	PA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160919-10	M Holdings Securities	OR	Banking/Credit/Financial	Yes - Published #	19,012
ITRC20160908-08	Merrimack Mortgage	NH	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160816-05	FSC Securities Corporation	GA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160816-04	First Home Mortgage Corp.	MD	Banking/Credit/Financial	Yes - Published #	1,300
ITRC20160809-09	Santander	MA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160809-03	TD Bank	NJ	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160711-05	TD Bank	NJ	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160628-05	TD Bank	NJ	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160621-03	Santa Rosa Consulting	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160614-17	Primary Residential Mortgage	UT	Banking/Credit/Financial	Yes - Published #	2,889
ITRC20160614-08	Nationwide Retirement Solutions	OH	Banking/Credit/Financial	Yes - Published #	457
ITRC20160531-07	Ameris Bank	FL	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160516-06	Southern Michigan Bank & Trust	MI	Banking/Credit/Financial	Yes - Published #	38,601
ITRC20160504-03	Charles Schwab	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160426-13	TD Bank	NJ	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160425-07	Ash Brokerage Firm	IN	Banking/Credit/Financial	Yes - Published #	423
ITRC20160404-04	Wells Fargo ATMs	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160324-10	Nation's Lending Corporation	OH	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160226-03	Coast Central Credit Union	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20160120-02	Rockland Trust	MA	Banking/Credit/Financial	Yes - Published #	2,182
ITRC20160120-01	Credit Union of the Berkshires	MA	Banking/Credit/Financial	Yes - Published #	2,200
ITRC20160119-02	HSBC Bank USA, N.A.	NY	Banking/Credit/Financial	Yes - Unknown #	Unknown

Totals for Category: Banking/Credit/Financial **# of Breaches: 52** **# of Records: 72,262**
% of Breaches: 4.8% **% of Records: 0.2%**

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Category: Business

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20161231-37	Seirus Innovation	CA	Business	Yes - Unknown #	Unknown
ITRC20161231-36	Tetra Technologies	TX	Business	Yes - Unknown #	Unknown
ITRC20161231-35	L4 Digital	WA	Business	Yes - Unknown #	Unknown
ITRC20161231-34	Numerex Corporation	GA	Business	Yes - Unknown #	Unknown
ITRC20161231-33	Maxim Crane Works	CA	Business	Yes - Unknown #	Unknown
ITRC20161231-32	Engineering Solutions & Products	VA	Business	Yes - Unknown #	Unknown
ITRC20161231-31	PayneWest Insurance	MT	Business	Yes - Unknown #	Unknown
ITRC20161231-29	Road and Highway Builders, LLC	NV	Business	Yes - Unknown #	Unknown
ITRC20161231-28	GlaxoSmithKline	PA	Business	Yes - Unknown #	Unknown
ITRC20161231-27	Armstrong, Backus & Co., LLP / myPay Solutions	TX	Business	Yes - Unknown #	Unknown
ITRC20161231-25	Next Generation Tax and Accounting	NE	Business	Yes - Unknown #	Unknown
ITRC20161231-24	Midland Paper Packaging & Supplies	IL	Business	Yes - Unknown #	Unknown
ITRC20161231-23	Rule Steel	ID	Business	Yes - Unknown #	Unknown
ITRC20161231-22	Pioneer News Group	WA	Business	Yes - Unknown #	Unknown
ITRC20161231-21	Prime Therapeutics	MN	Business	Yes - Unknown #	Unknown
ITRC20161231-20	Addus HomeCare	IL	Business	Yes - Unknown #	Unknown
ITRC20161231-19	Glu Mobile	CA	Business	Yes - Unknown #	Unknown
ITRC20161231-18	Leavitt Group	UT	Business	Yes - Unknown #	Unknown
ITRC20161231-17	Distinct Software Solutions dba Golf18Network	TX	Business	Yes - Unknown #	Unknown
ITRC20161231-16	MKK Consulting	CO	Business	Yes - Unknown #	Unknown
ITRC20161231-15	Curse, Inc.	AL	Business	Yes - Unknown #	Unknown
ITRC20161231-13	Southcentral Foundation	AK	Business	Yes - Unknown #	Unknown
ITRC20161231-09	Gustafson & Wargo, CPAs, LLP	NY	Business	Yes - Unknown #	Unknown
ITRC20161231-08	American Pharmacists Association / Comnet	DC	Business	Yes - Unknown #	Unknown
ITRC20161231-07	Hash, O'Brien, Biby & Murray PLLP	MT	Business	Yes - Unknown #	Unknown
ITRC20161231-06	Cascade Management, Inc.	OR	Business	Yes - Published #	3,465

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161231-02	Sheet Metal Workers' Local Union No. 104	CA	Business	Yes - Unknown #	Unknown
ITRC20161229-23	Venture Logistics	IN	Business	Yes - Unknown #	Unknown
ITRC20161229-21	Julep Beauty, Inc.	WA	Business	Yes - Unknown #	Unknown
ITRC20161229-20	Indique	MA	Business	Yes - Published #	1,500
ITRC20161229-19	Gorilla Glue Company	OH	Business	Yes - Unknown #	Unknown
ITRC20161229-18	Fujitsu Computer Products of America, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20161229-17	Breville USA	CA	Business	Yes - Unknown #	Unknown
ITRC20161229-15	Safe for Home Products LLC dba Naturepedic	OH	Business	Yes - Unknown #	Unknown
ITRC20161229-10	V.I. Pay, Inc.	MI	Business	Yes - Unknown #	Unknown
ITRC20161229-07	Graphik Dimensions, Ltd.	NC	Business	Yes - Unknown #	Unknown
ITRC20161229-06	Topps Company, Inc.	NY	Business	Yes - Unknown #	Unknown
ITRC20161229-03	InterContinental Hotels Group	GA	Business	Yes - Unknown #	Unknown
ITRC20161222-05	Bomberg, Roach & Hanson, PLLC	MN	Business	Yes - Unknown #	Unknown
ITRC20161221-05	Western Union Financial Services, Inc.	CO	Business	Yes - Published #	15,700
ITRC20161220-10	United States Fire Insurance Company	NJ	Business	Yes - Unknown #	Unknown
ITRC20161220-09	American College of Emergency Physicians / ComNet	TX	Business	Yes - Unknown #	Unknown
ITRC20161220-08	Taleff & Murphy, P.C.	MT	Business	Yes - Unknown #	Unknown
ITRC20161220-07	USAA Federal Savings Bank	TX	Business	Yes - Unknown #	Unknown
ITRC20161220-06	Green Plains, Inc.	NE	Business	Yes - Unknown #	Unknown
ITRC20161220-05	Anderson, Tackman & Company PLC	WI	Business	Yes - Unknown #	Unknown
ITRC20161220-04	Matouk Factory Store	MA	Business	Yes - Unknown #	Unknown
ITRC20161219-07	Lumiere Place Casino & Hotels / Tropicana St. Louis, L	MO	Business	Yes - Unknown #	Unknown
ITRC20161219-06	UnitedStatesGoldBureau.com	AL	Business	Yes - Unknown #	Unknown
ITRC20161219-03	Lynda.com	CA	Business	Yes - Unknown #	Unknown
ITRC20161219-02	Modern Business Solutions	TX	Business	Yes - Unknown #	Unknown
ITRC20161216-17	Coronado Stone Products	CA	Business	Yes - Unknown #	Unknown
ITRC20161216-12	Interstate Hotels & Resorts	VA	Business	Yes - Unknown #	Unknown
ITRC20161216-10	Applause App Quality, Inc.	MA	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161216-09	Plano Synergy	IL	Business	Yes - Unknown #	Unknown
ITRC20161216-08	Trop Gun Shop	PA	Business	Yes - Unknown #	Unknown
ITRC20161216-07	VBrick Systems, Inc.	VA	Business	Yes - Unknown #	Unknown
ITRC20161216-06	Acceptance Insurance	TN	Business	Yes - Unknown #	Unknown
ITRC20161216-05	O.C. Tanner	UT	Business	Yes - Unknown #	Unknown
ITRC20161216-02	Bleacher Report / Turner Broadcasting System	CA	Business	Yes - Unknown #	Unknown
ITRC20161215-05	K Partners Hotel Management	TX	Business	Yes - Unknown #	Unknown
ITRC20161215-01	Yahoo #2	CA	Business	Yes - Unknown #	Unknown
ITRC20161213-02	BraceAbility	IA	Business	Yes - Unknown #	Unknown
ITRC20161212-12	FriendFinders Network	CA	Business	Yes - Unknown #	Unknown
ITRC20161212-10	Total Community Options, Inc. dba InnovAge	CO	Business	Yes - Unknown #	Unknown
ITRC20161212-09	Raging Wire Data Centers	NV	Business	Yes - Unknown #	Unknown
ITRC20161212-08	Veterans Management Services, Inc.	VA	Business	Yes - Unknown #	Unknown
ITRC20161212-07	Avinger, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20161212-06	Symphony EYC	MA	Business	Yes - Unknown #	Unknown
ITRC20161212-05	Group Benefit Services	MD	Business	Yes - Unknown #	Unknown
ITRC20161212-04	Astreya Partners, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20161212-03	Westcor Land Title Insurance Company	FL	Business	Yes - Unknown #	Unknown
ITRC20161212-02	BlackHeart Records	NY	Business	Yes - Unknown #	Unknown
ITRC20161209-06	Citrix Systems	FL	Business	Yes - Unknown #	Unknown
ITRC20161206-11	Wisconsin National Guard Association	WI	Business	Yes - Unknown #	Unknown
ITRC20161206-10	Educents	CA	Business	Yes - Unknown #	Unknown
ITRC20161206-09	Caesars Entertainment	NV	Business	Yes - Unknown #	Unknown
ITRC20161206-08	Brennan Recupero Cascione Scungio and McAllister L	RI	Business	Yes - Unknown #	Unknown
ITRC20161206-07	BWTX Associates	TX	Business	Yes - Unknown #	Unknown
ITRC20161206-06	SwervePoint, LLC	MA	Business	Yes - Unknown #	Unknown
ITRC20161206-04	Guilmartin, DiPiro & Sokolowski, LLC	CT	Business	Yes - Unknown #	Unknown
ITRC20161205-13	TSYS Merchant Solutions	NE	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161205-11	LANG Companies	WI	Business	Yes - Unknown #	Unknown
ITRC20161205-10	Office of Hillary Tentler	CA	Business	Yes - Unknown #	Unknown
ITRC20161202-01	BLU	FL	Business	Yes - Published #	120,000
ITRC20161129-10	U.S. Olympic Committee	CO	Business	Yes - Unknown #	Unknown
ITRC20161129-09	IDEO.org	CA	Business	Yes - Unknown #	Unknown
ITRC20161129-07	Aon Hewitt	IL	Business	Yes - Published #	2,892
ITRC20161129-01	Spreadshirt.com	MA	Business	Yes - Unknown #	Unknown
ITRC20161128-21	AdultFriendFinder	CA	Business	Yes - Unknown #	Unknown
ITRC20161128-17	Office of Dale A. Wein, Prof. LLC	SD	Business	Yes - Unknown #	Unknown
ITRC20161128-15	Natural Life Collections, Inc.	FL	Business	Yes - Unknown #	Unknown
ITRC20161128-14	National Satellite Center	CA	Business	Yes - Unknown #	Unknown
ITRC20161128-13	Christian Louboutin	NY	Business	Yes - Unknown #	Unknown
ITRC20161128-12	Baker, Overby & Moore, Inc., P.S.	WA	Business	Yes - Unknown #	Unknown
ITRC20161128-11	State Farm	IL	Business	Yes - Unknown #	Unknown
ITRC20161128-10	Yummie by Heather Thomson	NY	Business	Yes - Unknown #	Unknown
ITRC20161128-08	Backcountry Gear	OR	Business	Yes - Unknown #	Unknown
ITRC20161122-08	Madison Square Garden Company	NY	Business	Yes - Unknown #	Unknown
ITRC20161122-02	Atlantis, Paradise Island (Brookfield Asset Managemen	FL	Business	Yes - Unknown #	Unknown
ITRC20161122-01	Springfield Armory	IL	Business	Yes - Unknown #	Unknown
ITRC20161121-04	Gray Television	GA	Business	Yes - Unknown #	Unknown
ITRC20161121-03	Odyssey Logistics & Technology Corporation	CT	Business	Yes - Unknown #	Unknown
ITRC20161118-12	MYR Group	IL	Business	Yes - Published #	6,878
ITRC20161118-04	Sirius XM	NY	Business	Yes - Unknown #	Unknown
ITRC20161118-02	QVC	PA	Business	Yes - Unknown #	Unknown
ITRC20161115-04	Windy Ridge Accounting & Tax Service	OR	Business	Yes - Unknown #	Unknown
ITRC20161115-03	Honig's Whistle Stop, Inc.	MI	Business	Yes - Unknown #	Unknown
ITRC20161115-01	Eileen Fisher	NY	Business	Yes - Unknown #	Unknown
ITRC20161109-01	UFCW Local 655	MO	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161108-04	Prime Inc.	MO	Business	Yes - Unknown #	Unknown
ITRC20161108-03	Morris Rothenberg & Son, Inc. dba Rothco	NY	Business	Yes - Unknown #	Unknown
ITRC20161108-02	DealerBuilt / Auto Dealerships Nationwide	IA	Business	Yes - Unknown #	Unknown
ITRC20161107-09	Sentinel Hotel	OR	Business	Yes - Unknown #	Unknown
ITRC20161107-08	Thirty Three Threads, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20161107-07	Manduka	CA	Business	Yes - Unknown #	Unknown
ITRC20161107-06	i-Dressup.com	US	Business	Yes - Unknown #	Unknown
ITRC20161107-05	Welk Resort Group	CA	Business	Yes - Unknown #	Unknown
ITRC20161107-04	National Wholesale Incorporated	NC	Business	Yes - Published #	14,281
ITRC20161101-02	Don Joses Mexican Restaurant	TX	Business	Yes - Unknown #	Unknown
ITRC20161031-16	Stream Gas & Electric	TX	Business	Yes - Unknown #	Unknown
ITRC20161031-15	Kolodzey & Cox CPAs, PC	NJ	Business	Yes - Unknown #	Unknown
ITRC20161031-14	Batdorf & Bronson Coffee Roasters	WA	Business	Yes - Published #	1,845
ITRC20161031-13	USI Insurance Services / Unifers Workplace Solutions	NY	Business	Yes - Published #	1,851
ITRC20161031-12	Oldcastle Building Envelope	GA	Business	Yes - Unknown #	Unknown
ITRC20161031-11	Mid-Ohio Foodbank	OH	Business	Yes - Unknown #	Unknown
ITRC20161031-10	Ben Bridge Jewelers	WA	Business	Yes - Unknown #	Unknown
ITRC20161031-06	Abernathy & Company	AR	Business	Yes - Unknown #	Unknown
ITRC20161031-04	New Leaders	NY	Business	Yes - Unknown #	Unknown
ITRC20161031-03	Politi & Magnifico LLC	CT	Business	Yes - Unknown #	Unknown
ITRC20161031-01	Beyond Yoga	CA	Business	Yes - Unknown #	Unknown
ITRC20161028-4	Spectrum, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20161028-06	Habitat for Humanity	MI	Business	Yes - Published #	5,500
ITRC20161028-05	Hill+Knowlton	NY	Business	Yes - Published #	592
ITRC20161028-03	Napoli Bern Ripka Shkolnik, LLP	NY	Business	Yes - Unknown #	Unknown
ITRC20161026-07	SOS International LLC	NY	Business	Yes - Unknown #	Unknown
ITRC20161026-06	ParsonsKellogg	RI	Business	Yes - Unknown #	Unknown
ITRC20161026-04	Atlanta Falcons Football Club, LLC / NCR Corporation	GA	Business	Yes - Published #	975

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161026-02	Medical Marijuana Dispensary	AZ	Business	Yes - Unknown #	Unknown
ITRC20161026-01	Cisco Systems	CA	Business	Yes - Unknown #	Unknown
ITRC20161025-02	TOPCON / Paychex	CA	Business	Yes - Unknown #	Unknown
ITRC20161024-16	Zero Gravity Solutions	FL	Business	Yes - Unknown #	Unknown
ITRC20161024-15	New America	CA	Business	Yes - Unknown #	Unknown
ITRC20161024-13	Smith, Patrick LLC	MO	Business	Yes - Published #	1,649
ITRC20161024-12	SportBrella	CA	Business	Yes - Unknown #	Unknown
ITRC20161024-11	Vacation Express USA Corp	GA	Business	Yes - Unknown #	Unknown
ITRC20161024-10	Water Environment Federation / Comnet Marketing Gr	VA	Business	Yes - Unknown #	Unknown
ITRC20161024-09	John J. Capelli, CPA	CA	Business	Yes - Unknown #	Unknown
ITRC20161024-08	Wyndham Vacation Resorts	NJ	Business	Yes - Unknown #	Unknown
ITRC20161024-07	KRT CPAs	GA	Business	Yes - Published #	3,793
ITRC20161024-06	Frank Day, CPA LLC	NY	Business	Yes - Unknown #	Unknown
ITRC20161024-03	Tom McLeod Software Corps	AL	Business	Yes - Unknown #	Unknown
ITRC20161024-01	Tricerat, Inc.	MD	Business	Yes - Unknown #	Unknown
ITRC20161021-04	Eastwood Company	PA	Business	Yes - Published #	20,929
ITRC20161021-02	Foursquare	NY	Business	Yes - Unknown #	Unknown
ITRC20161021-01	Weebly	CA	Business	Yes - Unknown #	Unknown
ITRC20161019-02	National Republican Senatorial Committee (NRSC) / Ta	DC	Business	Yes - Unknown #	Unknown
ITRC20161018-15	Chevron USA, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20161018-14	Big Y Foods	CT	Business	Yes - Unknown #	Unknown
ITRC20161018-13	Borden Perlman Salisbury & Kelly	NJ	Business	Yes - Unknown #	Unknown
ITRC20161018-12	Liberty Buy Sell	OR	Business	Yes - Unknown #	Unknown
ITRC20161018-11	Noble House - Teton Mountain Lodge & Spa / Hotel Ter	WA	Business	Yes - Unknown #	Unknown
ITRC20161018-01	Gibson Insurance Agency	IN	Business	Yes - Published #	7,242
ITRC20161014-15	Krispy Kreme Donut Corporation	NC	Business	Yes - Unknown #	Unknown
ITRC20161014-14	National Church Solutions	WV	Business	Yes - Unknown #	Unknown
ITRC20161014-13	Independent Medical Specialty Dealers Association / S	OH	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161014-11	Paul Stuart	NY	Business	Yes - Unknown #	Unknown
ITRC20161014-10	Pennsylvania Lumbermens Mutual Insurance Compan	PA	Business	Yes - Unknown #	Unknown
ITRC20161014-09	Rayner, Foos, Kruse and Irwin	OH	Business	Yes - Published #	1,336
ITRC20161014-08	Quikrete, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20161014-07	Higdon & Hale Certified Public Accountants	KS	Business	Yes - Unknown #	Unknown
ITRC20161014-06	Flynn & Company, Inc. Certified Public Accountants	OH	Business	Yes - Unknown #	Unknown
ITRC20161014-05	Washington County Housing and Redevelopment Auth	MD	Business	Yes - Unknown #	Unknown
ITRC20161014-03	Virginia Premier Health Plan	VA	Business	Yes - Unknown #	Unknown
ITRC20161014-02	Hogan Taylor, LLP	OK	Business	Yes - Unknown #	Unknown
ITRC20161013-23	MicroDAQ	NH	Business	Yes - Unknown #	Unknown
ITRC20161013-10	Hutchinson Community Foundation	KS	Business	Yes - Published #	5,500
ITRC20161013-09	Presnell Gage, PLLC	ID	Business	Yes - Published #	8,724
ITRC20161013-05	Vaupell	WA	Business	Yes - Published #	2,897
ITRC20161013-04	Vera Bradley, Inc.	IN	Business	Yes - Unknown #	Unknown
ITRC20161013-03	Qvale Auto Group, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20161013-02	Public Health Institute	CA	Business	Yes - Unknown #	Unknown
ITRC20161004-10	VF Outlet, Inc.	NC	Business	Yes - Unknown #	Unknown
ITRC20160929-07	Florida Bar Association	FL	Business	Yes - Unknown #	Unknown
ITRC20160929-05	Habitat for Humanity of Colorado	CO	Business	Yes - Unknown #	Unknown
ITRC20160929-03	Santoro CPA / Simplebooks Corp.	CT	Business	Yes - Unknown #	Unknown
ITRC20160929-01	Producteev / Jive Software	CA	Business	Yes - Unknown #	Unknown
ITRC20160927-04	Tully Automotive Group	NH	Business	Yes - Unknown #	Unknown
ITRC20160927-03	Scentlok Technologies	MI	Business	Yes - Published #	1,202
ITRC20160927-02	Specialty Equipment Market Association (SEMA) / Com	NJ	Business	Yes - Published #	490
ITRC20160926-01	Novation Settlement Solutions	FL	Business	Yes - Published #	Unknown
ITRC20160923-13	EMR4all, Inc. / Rehab Billing Solutions	CA	Business	Yes - Unknown #	Unknown
ITRC20160923-12	Regpack / BlueSnap	CA	Business	Yes - Unknown #	Unknown
ITRC20160923-04	Yahoo	CA	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160923-02	Stallcup & Associates, CPAs	CA	Business	Yes - Unknown #	Unknown
ITRC20160922-03	Genghis Grills	TX	Business	Yes - Unknown #	Unknown
ITRC20160920-10	UIL Holdings Corporation	CT	Business	Yes - Published #	116
ITRC20160920-08	Masy BioServices / Masy Systems, Inc.	MA	Business	Yes - Published #	145
ITRC20160920-07	FraserCPA	NJ	Business	Yes - Unknown #	Unknown
ITRC20160920-06	Hickey Law Firm	FL	Business	Yes - Unknown #	Unknown
ITRC20160920-05	Man Alive, Inc. / Lane Treatment Center	MD	Business	Yes - Unknown #	Unknown
ITRC20160920-04	ClixSense	NC	Business	Yes - Unknown #	Unknown
ITRC20160919-13	Ursus Holdings	TX	Business	Yes - Unknown #	Unknown
ITRC20160919-12	Menzies Aviation, Inc. 401(k) plan / Ascensus, Inc.	PA	Business	Yes - Unknown #	Unknown
ITRC20160919-11	Rebecca Minkoff	NY	Business	Yes - Published #	6,855
ITRC20160919-08	Lulu's Fashion Lounge	CA	Business	Yes - Unknown #	Unknown
ITRC20160915-03	Office of Michelle A. Pecora CPA	OR	Business	Yes - Unknown #	Unknown
ITRC20160915-02	Wheeler & Egger	CA	Business	Yes - Unknown #	Unknown
ITRC20160908-07	Exterran	TX	Business	Yes - Published #	10,844
ITRC20160908-06	Jerry's Artarama N.C., Inc.	NC	Business	Yes - Unknown #	Unknown
ITRC20160908-04	Nourse Farms	MA	Business	Yes - Published #	6,320
ITRC20160907-07	Stand Up Desk Store (SUDS)	AL	Business	Yes - Unknown #	Unknown
ITRC20160907-06	Vulcan Industries	AL	Business	Yes - Unknown #	Unknown
ITRC20160907-03	New York State Psychiatric Institute	NY	Business	Yes - Published #	21,880
ITRC20160906-03	Hutton Hotel	TN	Business	Yes - Unknown #	Unknown
ITRC20160906-01	Dropbox	CA	Business	Yes - Unknown #	Unknown
ITRC20160830-09	W.C. Ralston Architects	VA	Business	Yes - Unknown #	Unknown
ITRC20160830-08	J. Polep Distribution Services	MA	Business	Yes - Unknown #	Unknown
ITRC20160830-07	Dennis Group	MA	Business	Yes - Unknown #	Unknown
ITRC20160830-06	Birch Communications	CA	Business	Yes - Published #	1,913
ITRC20160830-05	Millenium Hotels & Resorts	CO	Business	Yes - Unknown #	Unknown
ITRC20160829-04	Liberty Mountain Sports, LLC	UT	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160829-03	Noble House Hotels & Resorts - Ocean Key Resort & S	WA	Business	Yes - Unknown #	Unknown
ITRC20160829-02	Toyota Motor Credit Corporation	CA	Business	Yes - Published #	8,989
ITRC20160825-04	Burke Mountain	VT	Business	Yes - Unknown #	Unknown
ITRC20160825-02	Precision Pipeline, LLC	WI	Business	Yes - Published #	3,675
ITRC20160825-01	Penn State Alumni Association / ComNet Marketing Gr	PA	Business	Yes - Unknown #	Unknown
ITRC20160824-15	SocialBlade	US	Business	Yes - Unknown #	Unknown
ITRC20160824-10	Factory RV Surplus	IN	Business	Yes - Published #	8,500
ITRC20160824-04	Epic Games	NC	Business	Yes - Unknown #	Unknown
ITRC20160824-02	Schwan's	MN	Business	Yes - Unknown #	Unknown
ITRC20160824-01	Eddie Bauer, LLC	WA	Business	Yes - Published #	2,192,422
ITRC20160816-06	Shoppe Designs	CA	Business	Yes - Unknown #	Unknown
ITRC20160816-03	EBSCO Industries, Inc.	AL	Business	Yes - Unknown #	Unknown
ITRC20160815-04	HEI Hotels & Resorts	CT	Business	Yes - Unknown #	Unknown
ITRC20160815-03	PAX Labs, Inc.	CA	Business	Yes - Published #	6,036
ITRC20160815-01	7-Eleven, Inc.	CA	Business	Yes - Published #	7,832
ITRC20160809-08	KGA, Inc.	MA	Business	Yes - Unknown #	Unknown
ITRC20160809-07	Primoris Services Corporation / Hein & Associates LLP	CO	Business	Yes - Unknown #	Unknown
ITRC20160809-02	MedAltus. LLC	NY	Business	Yes - Unknown #	Unknown
ITRC20160809-01	Travelon	IL	Business	Yes - Published #	1,672
ITRC20160808-01	Oracle - MICROS	CA	Business	Yes - Unknown #	Unknown
ITRC20160802-33	Institute of Management Accountants	NJ	Business	Yes - Unknown #	Unknown
ITRC20160802-32	Comnet Marketing Group	OR	Business	Yes - Unknown #	Unknown
ITRC20160802-31	Tax Shack	WA	Business	Yes - Unknown #	Unknown
ITRC20160802-30	NLU Products / BGZ Brands	UT	Business	Yes - Published #	114,261
ITRC20160802-29	Academy of Nutrition and Dietetics	IL	Business	Yes - Unknown #	Unknown
ITRC20160802-28	American Society of Safety Engineers	IL	Business	Yes - Unknown #	Unknown
ITRC20160802-27	Internet Chess Club	PA	Business	Yes - Published #	1,651
ITRC20160802-24	Democratic Political Organizations	DC	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160802-15	Kimpton Hotels	CA	Business	Yes - Unknown #	Unknown
ITRC20160802-05	Disney Consumer Products / Playdom Forum	CA	Business	Yes - Unknown #	Unknown
ITRC20160719-17	USA Field Hockey	CO	Business	Yes - Unknown #	Unknown
ITRC20160719-15	American Association for the Advancement of Science	DC	Business	Yes - Unknown #	Unknown
ITRC20160719-08	San Antonio Shoemakers (SAS)	TX	Business	Yes - Published #	50,000
ITRC20160719-07	IAP - Ingenuity and Purpose	FL	Business	Yes - Published #	4,272
ITRC20160719-06	North Palm Motors	FL	Business	Yes - Published #	22,961
ITRC20160719-05	Matador Recordings dba Madador Direct	NY	Business	Yes - Unknown #	Unknown
ITRC20160719-04	Opes Advisors	CA	Business	Yes - Unknown #	Unknown
ITRC20160719-03	Project Management Institute / Comnet Marketing Gro	PA	Business	Yes - Published #	9,100
ITRC20160708-01	Omni Hotels and Resorts	TX	Business	Yes - Published #	50,000
ITRC20160705-04	KontrolFreek, LLC	GA	Business	Yes - Unknown #	Unknown
ITRC20160705-03	Kool Kids Model & Talent Management	CA	Business	Yes - Unknown #	Unknown
ITRC20160628-04	Benchmark Senior Living	MA	Business	Yes - Published #	218
ITRC20160628-02	Gamesa Wind US, LLC	PA	Business	Yes - Unknown #	Unknown
ITRC20160628-01	SP+ Municipal Services	MD	Business	Yes - Unknown #	Unknown
ITRC20160627-03	Sageworks, Inc.	NC	Business	Yes - Unknown #	Unknown
ITRC20160627-02	Hard Rock Hotel & Casino Las Vegas	NV	Business	Yes - Unknown #	Unknown
ITRC20160621-05	Washington Redskins	DC	Business	Yes - Unknown #	Unknown
ITRC20160621-04	State Farm Mutual Automobile Insurance Company	IL	Business	Yes - Unknown #	Unknown
ITRC20160621-01	Crane Payment Innovations, Inc.	PA	Business	Yes - Unknown #	Unknown
ITRC20160620-09	GoToMyPC	CA	Business	Yes - Unknown #	Unknown
ITRC20160620-06	TieMart, Inc.	IL	Business	Yes - Published #	927
ITRC20160620-05	Sandler & Travis Trade Advisory Services, LLC	DC	Business	Yes - Unknown #	Unknown
ITRC20160620-01	Multi-Color Corporation	OH	Business	Yes - Published #	4,602
ITRC20160614-16	EPTAM Plastics	NH	Business	Yes - Unknown #	Unknown
ITRC20160614-13	Quarles & Brady, LLP	WI	Business	Yes - Published #	1,032
ITRC20160614-04	SD Associates, P.C.	PA	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160614-03	Cohen & Grieb, P.A.	FL	Business	Yes - Unknown #	Unknown
ITRC20160614-02	Acer Service Corporation	TX	Business	Yes - Published #	34,500
ITRC20160610-01	State Farm / DAC Group	IL	Business	Yes - Published #	7,570
ITRC20160607-13	Single Digits	NH	Business	Yes - Unknown #	Unknown
ITRC20160607-12	Match-Up Solutions, LLC	FL	Business	Yes - Published #	3,078
ITRC20160607-07	Sun Road	FL	Business	Yes - Unknown #	Unknown
ITRC20160607-06	CiCi's Pizza	TX	Business	Yes - Unknown #	Unknown
ITRC20160607-01	Empathia, Inc.	CA	Business	Yes - Published #	26,446
ITRC20160601-06	Tumblr	NY	Business	Yes - Unknown #	Unknown
ITRC20160601-05	Myspace	CA	Business	Yes - Unknown #	Unknown
ITRC20160601-04	National Network of Abortion Funds	MA	Business	Yes - Unknown #	Unknown
ITRC20160601-02	Shoes West Distribution Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20160531-09	AIM Inc.	IL	Business	Yes - Unknown #	Unknown
ITRC20160531-06	Macfadden	MD	Business	Yes - Unknown #	Unknown
ITRC20160524-12	ABCya.com	RI	Business	Yes - Unknown #	Unknown
ITRC20160524-09	Puppet, Inc.	TX	Business	Yes - Unknown #	Unknown
ITRC20160524-08	Milwaukee Bucks	WI	Business	Yes - Unknown #	Unknown
ITRC20160524-07	Maritz Holdings, Inc.	MO	Business	Yes - Published #	1,871
ITRC20160524-06	A&A Ready Mixed Concrete, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20160524-02	Noodles & Company	CO	Business	Yes - Unknown #	Unknown
ITRC20160524-01	O'Charley's Restaurants	GA	Business	Yes - Unknown #	Unknown
ITRC20160523-04	Conway Group, Inc.	MD	Business	Yes - Unknown #	Unknown
ITRC20160523-03	Paper Works	CA	Business	Yes - Unknown #	Unknown
ITRC20160523-02	Flurish, Inc. dba LendUp	CA	Business	Yes - Unknown #	Unknown
ITRC20160523-01	H&R Block	MO	Business	Yes - Unknown #	Unknown
ITRC20160517-04	Digilant	MA	Business	Yes - Unknown #	Unknown
ITRC20160516-03	NTT Data	TX	Business	Yes - Published #	1,493
ITRC20160513-06	RugDoctor	TX	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160513-04	Avention (formerly OneSourceSolutions)	MA	Business	Yes - Unknown #	Unknown
ITRC20160513-01	Office of Lynn N. Talbott, Jr. CPA	CA	Business	Yes - Unknown #	Unknown
ITRC20160512-07	ADP	NJ	Business	Yes - Unknown #	Unknown
ITRC20160510-02	Strafaci & Associates	FL	Business	Yes - Unknown #	Unknown
ITRC20160510-01	New Hampshire Distributors	NH	Business	Yes - Unknown #	Unknown
ITRC20160509-10	Pure Integration, LLC	VA	Business	Yes - Unknown #	Unknown
ITRC20160509-06	Nordic Consulting Partners / NavigateHCR	UT	Business	Yes - Published #	1,209
ITRC20160509-05	Sanctuary Clothing	CA	Business	Yes - Unknown #	Unknown
ITRC20160509-04	CertifiKid	MD	Business	Yes - Published #	32,388
ITRC20160509-03	Bay Area Children's Association	CA	Business	Yes - Unknown #	Unknown
ITRC20160509-02	Stonebridge Realty Advisors, Inc. / Xebec restaurant	CA	Business	Yes - Unknown #	Unknown
ITRC20160509-01	Google	CA	Business	Yes - Unknown #	Unknown
ITRC20160506-02	Kroger / Equifax W-2 Express	GA	Business	Yes - Published #	431,000
ITRC20160505-03	Hume Lake Christian Camps	CA	Business	Yes - Unknown #	Unknown
ITRC20160505-02	Pro Sports Daily	IL	Business	Yes - Unknown #	Unknown
ITRC20160505-01	Lafler Moore Connerty & Webb	CA	Business	Yes - Unknown #	Unknown
ITRC20160504-02	Office of Ken Waterman CPA PC	CA	Business	Yes - Unknown #	Unknown
ITRC20160504-01	Areas	FL	Business	Yes - Published #	4,362
ITRC20160503-19	YourEncore, Inc.	IN	Business	Yes - Unknown #	Unknown
ITRC20160503-18	Union League Club of Chicago	IL	Business	Yes - Unknown #	Unknown
ITRC20160503-17	Tiger Leasing	NY	Business	Yes - Unknown #	Unknown
ITRC20160503-15	MMF Industries (Block and Company, Inc.)	MI	Business	Yes - Unknown #	Unknown
ITRC20160503-14	Home for Little Wanderers	MA	Business	Yes - Unknown #	Unknown
ITRC20160503-13	Hi-Tec	CA	Business	Yes - Published #	1,603
ITRC20160503-12	HAECO Americas	NC	Business	Yes - Unknown #	Unknown
ITRC20160503-11	Draper James	TN	Business	Yes - Unknown #	Unknown
ITRC20160503-10	Avendra, LLC	MD	Business	Yes - Unknown #	Unknown
ITRC20160503-05	Alpha Payroll Services, LLC	PA	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160503-04	Brunswick Corporation / Mercury Marine	IL	Business	Yes - Published #	13,000
ITRC20160503-02	South Loop CPA	IL	Business	Yes - Unknown #	Unknown
ITRC20160429-11	TTI Floor Care North America	OH	Business	Yes - Unknown #	Unknown
ITRC20160429-10	Gryphon Technologies, LC	DC	Business	Yes - Unknown #	Unknown
ITRC20160429-09	BloomReach, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20160429-07	American Dental Association (ADA)	IL	Business	Yes - Unknown #	Unknown
ITRC20160429-05	Michels Corporation	WI	Business	Yes - Published #	8,161
ITRC20160429-04	GoldKey/PHR	VA	Business	Yes - Unknown #	Unknown
ITRC20160429-03	Geltrude & Company, LLC	NJ	Business	Yes - Unknown #	Unknown
ITRC20160429-02	Advance International Marketing (AIM)	NC	Business	Yes - Published #	63,888
ITRC20160429-01	LuckyPet	WA	Business	Yes - Published #	11,333
ITRC20160427-01	BeautifulPeople	NY	Business	Yes - Unknown #	Unknown
ITRC20160426-14	Trinity Heating & Air, Inc. dba Trinity Solar	NJ	Business	Yes - Published #	1,156
ITRC20160426-11	NetBrain Technologies, Inc.	MA	Business	Yes - Unknown #	Unknown
ITRC20160426-09	Landstar System, Inc.	FL	Business	Yes - Published #	1,362
ITRC20160426-08	Eastern Benefits Group	MA	Business	Yes - Unknown #	Unknown
ITRC20160426-07	Client Network Services, Inc.	MD	Business	Yes - Unknown #	Unknown
ITRC20160426-06	Behavioral Science Technology	CA	Business	Yes - Unknown #	Unknown
ITRC20160426-05	Agenus	MA	Business	Yes - Unknown #	Unknown
ITRC20160426-04	Fruitful Yield	IL	Business	Yes - Published #	3,921
ITRC20160426-03	Spotify	CA	Business	Yes - Unknown #	Unknown
ITRC20160425-15	TMEIC Corporation	VA	Business	Yes - Published #	300
ITRC20160425-14	Wynden Stark, dba GQR Global Markets/City Internshi	NY	Business	Yes - Unknown #	Unknown
ITRC20160425-13	OpSec	PA	Business	Yes - Unknown #	Unknown
ITRC20160425-12	Morongo Casino	CA	Business	Yes - Unknown #	Unknown
ITRC20160425-11	DealerSocket, Inc.	CA	Business	Yes - Published #	1,350
ITRC20160425-10	General Fasteners Company (MNP)	MI	Business	Yes - Published #	1,505
ITRC20160425-08	BackOffice Associates	MA	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160425-04	Grand Sierra Resort / (MEI-GSR)	NV	Business	Yes - Published #	156,508
ITRC20160421-11	Voya Financial Advisors, Inc.	NY	Business	Yes - Unknown #	Unknown
ITRC20160421-10	UFC Gym	CA	Business	Yes - Unknown #	Unknown
ITRC20160421-05	Pacific Gas and Electric Company	CA	Business	Yes - Published #	2,426
ITRC20160421-01	Oneida Health Center Dental Clinic	WI	Business	Yes - Published #	2,734
ITRC20160420-05	InvenSense, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20160420-02	Archdiocese of Denver	CO	Business	Yes - Published #	18,000
ITRC20160419-01	DoTERRA	UT	Business	Yes - Unknown #	Unknown
ITRC20160418-16	Office of Virgil Elliot Winn, CPA	SC	Business	Yes - Unknown #	Unknown
ITRC20160418-15	Silicon Laboratories, Inc.	TX	Business	Yes - Unknown #	Unknown
ITRC20160418-14	Proskauer Rose LLP	NY	Business	Yes - Unknown #	Unknown
ITRC20160418-13	O'Reilly Media Group	CA	Business	Yes - Unknown #	Unknown
ITRC20160418-12	OnDeck Capital, Inc.	NY	Business	Yes - Published #	1,570
ITRC20160418-10	Dixie Group	CA	Business	Yes - Unknown #	Unknown
ITRC20160418-09	Asure Software	TX	Business	Yes - Unknown #	Unknown
ITRC20160418-08	Money Now	KY	Business	Yes - Unknown #	Unknown
ITRC20160418-06	Girl Scouts of Gulfcoast Florida, Inc.	FL	Business	Yes - Unknown #	Unknown
ITRC20160418-04	Examination Management Services, Inc. (EMSI)	TX	Business	Yes - Published #	4,965
ITRC20160418-01	WLNE-TV	RI	Business	Yes - Unknown #	Unknown
ITRC20160415-02	American College of Cardiology (ACC)	DC	Business	Yes - Unknown #	Unknown
ITRC20160412-04	Schwaab, Inc. (Discount Rubber Stamps.com)	WI	Business	Yes - Published #	85,000
ITRC20160412-03	Staminus Communications	CA	Business	Yes - Published #	3,338
ITRC20160412-02	Bristol Farms	CA	Business	Yes - Unknown #	Unknown
ITRC20160408-02	Wallys Wine and Spirits	CA	Business	Yes - Unknown #	Unknown
ITRC20160408-01	Whiting Turner Contracting Company	MD	Business	Yes - Published #	5,904
ITRC20160406-07	Norfolk Admirals	VA	Business	Yes - Unknown #	Unknown
ITRC20160406-03	NRT	NJ	Business	Yes - Unknown #	Unknown
ITRC20160406-02	Universal Service Administrative Company (USAC)	DC	Business	Yes - Published #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160406-01	Katherman Kitts & Co.	CA	Business	Yes - Published #	1,407
ITRC20160405-10	Mohawk Mountain Ski Area	CT	Business	Yes - Unknown #	Unknown
ITRC20160405-09	Traphagen & Traphagen CPAs	NJ	Business	Yes - Unknown #	Unknown
ITRC20160405-08	Champlain Oil	VT	Business	Yes - Unknown #	Unknown
ITRC20160405-06	ARC International North America, LLC	NJ	Business	Yes - Unknown #	Unknown
ITRC20160405-01	Information Resources, Inc.	IL	Business	Yes - Published #	1,297
ITRC20160404-01	Trump Hotels	NY	Business	Yes - Unknown #	Unknown
ITRC20160401-02	Pivotal Software, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20160401-01	Ullrich Delevati	CA	Business	Yes - Unknown #	Unknown
ITRC20160329-06	Community in Action	GA	Business	Yes - Unknown #	Unknown
ITRC20160329-05	Ryman Hospitality Properties	TN	Business	Yes - Published #	2,478
ITRC20160328-01	Aspiranet	CA	Business	Yes - Unknown #	Unknown
ITRC20160324-13	Netcracker Technology Corporation	MA	Business	Yes - Unknown #	Unknown
ITRC20160324-12	Medieval Times	CA	Business	Yes - Unknown #	Unknown
ITRC20160324-11	QTI Group	WI	Business	Yes - Unknown #	Unknown
ITRC20160324-09	Century Fence	WI	Business	Yes - Unknown #	Unknown
ITRC20160324-08	Aspect	AZ	Business	Yes - Published #	1,300
ITRC20160324-07	Kantar Group (TNS)	NY	Business	Yes - Published #	28,000
ITRC20160324-06	ISCO Industries, Inc.	KY	Business	Yes - Published #	180
ITRC20160324-05	Verizon Enterprise Solutions	NJ	Business	Yes - Published #	1,500,000
ITRC20160324-04	Abel Womack	MA	Business	Yes - Unknown #	Unknown
ITRC20160324-03	Lamps Plus / Pacific Coast Lighting	CA	Business	Yes - Unknown #	Unknown
ITRC20160323-02	Dynamic Aviation	VA	Business	Yes - Unknown #	Unknown
ITRC20160322-08	Sirius XM	DC	Business	Yes - Published #	165
ITRC20160322-07	Lanyon Solutions, Inc.	TX	Business	Yes - Unknown #	Unknown
ITRC20160322-02	Sprouts	AZ	Business	Yes - Published #	21,000
ITRC20160322-01	ConvaTec, Inc.	NJ	Business	Yes - Unknown #	Unknown
ITRC20160321-13	Springfield City Utilities	MO	Business	Yes - Published #	1,000

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160321-12	Moneytree	WA	Business	Yes - Unknown #	Unknown
ITRC20160321-11	Foss Manufacturing Company, LLC	NH	Business	Yes - Unknown #	Unknown
ITRC20160321-10	SalientCRGT	VA	Business	Yes - Published #	1,192
ITRC20160321-08	Advance Auto Parts	VA	Business	Yes - Unknown #	Unknown
ITRC20160321-07	SevOne	MA	Business	Yes - Unknown #	Unknown
ITRC20160321-06	WorkCare, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20160318-01	PerkinElmer	AL	Business	Yes - Published #	2,738
ITRC20160315-15	LAZ Parking	CT	Business	Yes - Published #	14,000
ITRC20160315-14	GreenShades / Multiple entities	FL	Business	Yes - Unknown #	Unknown
ITRC20160315-12	Acronis, Inc.	MA	Business	Yes - Unknown #	Unknown
ITRC20160315-11	DataXu	MA	Business	Yes - Published #	318
ITRC20160315-08	MROStop LLC	NC	Business	Yes - Unknown #	Unknown
ITRC20160315-06	Applied Systems	IL	Business	Yes - Published #	1,206
ITRC20160315-05	Lewis Kisch and Associates Ltd.	MN	Business	Yes - Unknown #	Unknown
ITRC20160315-04	Information Innovators Inc.	VA	Business	Yes - Unknown #	Unknown
ITRC20160315-03	Matrix North American Construction	IL	Business	Yes - Published #	4,650
ITRC20160315-02	Care.com	MA	Business	Yes - Unknown #	Unknown
ITRC20160315-01	Laborers Funds Administrative Office of Northern Calif	CA	Business	Yes - Published #	2,373
ITRC20160314-02	Mitchell International, Inc.	CA	Business	Yes - Published #	1,648
ITRC20160314-01	1-800-Flowers.com	NY	Business	Yes - Unknown #	Unknown
ITRC20160308-06	GCI / General Communication, Inc.	AK	Business	Yes - Unknown #	Unknown
ITRC20160308-05	Adreima	IL	Business	Yes - Unknown #	Unknown
ITRC20160308-04	Microf LLC	GA	Business	Yes - Unknown #	Unknown
ITRC20160308-03	Turner Construction Company	NY	Business	Yes - Published #	9,841
ITRC20160307-08	Mansueto Ventures Inc. / Fast Company magazines	NY	Business	Yes - Unknown #	Unknown
ITRC20160307-07	Seagate	CA	Business	Yes - Published #	8,292
ITRC20160304-03	Billy Casper Golf	VA	Business	Yes - Published #	8,176
ITRC20160304-02	Evening Post Industries	SC	Business	Yes - Published #	2,314

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160304-01	Rosen Hotels and Resorts	FL	Business	Yes - Unknown #	Unknown
ITRC20160303-10	Actifio, Inc.	MA	Business	Yes - Unknown #	Unknown
ITRC20160303-09	AmeriPride Services, Inc.	MN	Business	Yes - Unknown #	Unknown
ITRC20160303-07	Cox Communications	GA	Business	Yes - Unknown #	Unknown
ITRC20160303-02	Robert Rauschenberg Foundation	NY	Business	Yes - Unknown #	Unknown
ITRC20160303-01	Pharm-Olam International	TX	Business	Yes - Unknown #	Unknown
ITRC20160302-01	Central Concrete Supply Co.	CA	Business	Yes - Unknown #	Unknown
ITRC20160301-03	Snapchat	CA	Business	Yes - Unknown #	Unknown
ITRC20160301-02	TN Marketing	MN	Business	Yes - Published #	13,118
ITRC20160226-05	Office of Allen Park, Attorney	MI	Business	Yes - Unknown #	Unknown
ITRC20160226-01	Sterbick & Associates, P.S.	WA	Business	Yes - Unknown #	Unknown
ITRC20160225-04	Mercy Housing, Inc. / Mercy Housing Management Gro	CO	Business	Yes - Unknown #	Unknown
ITRC20160225-03	Rightside	WA	Business	Yes - Unknown #	Unknown
ITRC20160223-04	Incipio, LLC	CA	Business	Yes - Unknown #	Unknown
ITRC20160223-03	EWTN Global Catholic Network	AL	Business	Yes - Published #	425
ITRC20160222-01	uKnowKids	VA	Business	Yes - Published #	1,740
ITRC20160218-01	Polycom	CA	Business	Yes - Unknown #	Unknown
ITRC20160217-02	Calpine Corporation	TX	Business	Yes - Unknown #	Unknown
ITRC20160216-03	Kankakee Valley REMC (Rutherford Electric Membersh	IN	Business	Yes - Published #	17,700
ITRC20160211-03	Capezio	NY	Business	Yes - Unknown #	Unknown
ITRC20160211-02	Superior Labels / RubberStamps.Net	IA	Business	Yes - Published #	7,000
ITRC20160211-01	Brightview (formerly Brickman Group, Ltd. LLC)	MD	Business	Yes - Published #	730
ITRC20160208-02	Baja Bound Insurance Services, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20160208-01	GYFT	CA	Business	Yes - Unknown #	Unknown
ITRC20160204-05	Clarks Americas, Inc.	MA	Business	Yes - Unknown #	Unknown
ITRC20160204-04	Oak Hill Citgo Gas & Convenience	ME	Business	Yes - Unknown #	Unknown
ITRC20160204-03	Phillip Capital, Inc.	IL	Business	Yes - Unknown #	Unknown
ITRC20160203-03	Berks & Beyond Employment Services	PA	Business	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20160203-02	Crest Foods	OK	Business	Yes - Unknown #	Unknown
ITRC20160203-01	Richardson & Company, P.C.	MA	Business	Yes - Unknown #	Unknown
ITRC20160202-01	International Alliance of Theatrical Stage Employees #	CA	Business	Yes - Unknown #	Unknown
ITRC20160201-14	Shannon Tax & Business Services	NM	Business	Yes - Unknown #	Unknown
ITRC20160201-13	cPanel	TX	Business	Yes - Unknown #	Unknown
ITRC20160201-05	Wendy's	OH	Business	Yes - Unknown #	Unknown
ITRC20160201-04	Alba Botanica	NY	Business	Yes - Unknown #	Unknown
ITRC20160201-03	LifeSafer	OH	Business	Yes - Unknown #	Unknown
ITRC20160201-02	TaxSlayer	GA	Business	Yes - Published #	8,800
ITRC20160201-01	Neiman Marcus Group	TX	Business	Yes - Published #	5,200
ITRC20160126-05	Baileys, Inc.	CA	Business	Yes - Published #	250,000
ITRC20160126-03	RealSelf, Inc.	WA	Business	Yes - Unknown #	Unknown
ITRC20160126-02	Kicky Pants, Inc.	CA	Business	Yes - Unknown #	Unknown
ITRC20160122-01	Blue Dolphin	CT	Business	Yes - Unknown #	Unknown
ITRC20160120-05	Bevo POS	FL	Business	Yes - Published #	799
ITRC20160120-03	Mrs. Fields Gifts	CO	Business	Yes - Published #	1,769
ITRC20160119-05	TaxAct / Blucora, Inc.	IA	Business	Yes - Published #	450
ITRC20160119-04	JB Autosports	IA	Business	Yes - Published #	1,000
ITRC20160119-03	RateMyProfessors.com	NY	Business	Yes - Unknown #	Unknown
ITRC20160108-04	Time Warner Cable	TX	Business	Yes - Unknown #	Unknown
ITRC20160105-01	Regional Income Tax Authority	OH	Business	Yes - Published #	50,000

Totals for Category: **Business**

of Breaches: 495 # of Records: 5,669,711
 % of Breaches: 45.3 % of Records: 15.5%

Category: Educational

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20161231-11	Career Education Corporation	IL	Educational	Yes - Unknown #	Unknown
ITRC20161231-10	Teikyo Loretto Heights University dba Colorado Height	CO	Educational	Yes - Unknown #	Unknown
ITRC20161230-01	Columbia County School District	GA	Educational	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161229-14	Georgia Tech	GA	Educational	Yes - Unknown #	Unknown
ITRC20161229-12	University of Maine	ME	Educational	Yes - Published #	86
ITRC20161229-05	Claremont University Consortium	CA	Educational	Yes - Unknown #	Unknown
ITRC20161222-04	Luther College	IA	Educational	Yes - Unknown #	Unknown
ITRC20161221-03	Columbia County School District	GA	Educational	Yes - Unknown #	Unknown
ITRC20161221-01	University of Nebraska - Lincoln	NE	Educational	Yes - Published #	30,000
ITRC20161219-05	Corpus Christi Independent School District	TX	Educational	Yes - Published #	443
ITRC20161216-15	Harvey Mudd College / Ultimate Software	CA	Educational	Yes - Unknown #	Unknown
ITRC20161216-11	Lynn University	FL	Educational	Yes - Unknown #	Unknown
ITRC20161216-03	Black Hawk College / Summit Reinsurance Services, In	IL	Educational	Yes - Published #	1,000
ITRC20161216-01	Frederick County Public Schools	MD	Educational	Yes - Published #	1,000
ITRC20161212-13	University of Wisconsin - Madison	WI	Educational	Yes - Published #	1,123
ITRC20161209-07	University of Vermont	VT	Educational	Yes - Unknown #	Unknown
ITRC20161206-05	Baylor College of Medicine	TX	Educational	Yes - Unknown #	Unknown
ITRC20161205-12	San Jose Evergreen Community College District	CA	Educational	Yes - Unknown #	Unknown
ITRC20161205-01	Chesapeake Public Schools	VA	Educational	Yes - Published #	10,827
ITRC20161128-16	University of Montana	MT	Educational	Yes - Unknown #	Unknown
ITRC20161128-03	Bigfork School District	MT	Educational	Yes - Unknown #	Unknown
ITRC20161121-02	Michigan State University	MI	Educational	Yes - Published #	400,000
ITRC20161118-10	Buffalo Public School District	NY	Educational	Yes - Published #	4,400
ITRC20161118-03	Chicago Public Schools	IL	Educational	Yes - Published #	30,000
ITRC20161028-01	Marymount University	VA	Educational	Yes - Unknown #	Unknown
ITRC20161026-03	Beford County Board of Education	TN	Educational	Yes - Published #	862
ITRC20161024-02	Grand Valley State University	MI	Educational	Yes - Published #	3,198
ITRC20161018-16	Delta Career Education Corpotation	VA	Educational	Yes - Published #	4,014
ITRC20161017-01	Katy Independent School District / SunGard K-12	TX	Educational	Yes - Published #	78,000
ITRC20161013-21	New Horizons Computer Learning Centers South Flori	FL	Educational	Yes - Unknown #	Unknown
ITRC20161004-01	Winston Dillard School Distric No. 116	OR	Educational	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160923-03	UC San Diego School of Medicine	CA	Educational	Yes - Unknown #	Unknown
ITRC20160920-02	La Joya American Federation of Teachers	TX	Educational	Yes - Unknown #	Unknown
ITRC20160907-08	University of Alaska Mat-Su Campus	AK	Educational	Yes - Published #	5,416
ITRC20160830-03	Langston Hughes Young Explorers Academy	NY	Educational	Yes - Unknown #	Unknown
ITRC20160824-12	University of New Mexico	NM	Educational	Yes - Published #	1,300
ITRC20160815-08	University of Vermont	VT	Educational	Yes - Unknown #	Unknown
ITRC20160802-07	University of North Carolina - Charlotte	NC	Educational	Yes - Unknown #	Unknown
ITRC20160719-01	KUSC / University of Southern California / Comnet Mar	CA	Educational	Yes - Unknown #	Unknown
ITRC20160711-03	North Carolina State University	NC	Educational	Yes - Published #	38,976
ITRC20160705-05	Capella University	MN	Educational	Yes - Unknown #	Unknown
ITRC20160628-06	Holley Central School District	NY	Educational	Yes - Unknown #	Unknown
ITRC20160615-02	University of Connecticut - School of Engineering	CT	Educational	Yes - Unknown #	Unknown
ITRC20160614-15	Bucknell University	PA	Educational	Yes - Unknown #	Unknown
ITRC20160608-01	Concord School District	NH	Educational	Yes - Unknown #	Unknown
ITRC20160607-05	Pennsylvania State University	PA	Educational	Yes - Published #	379
ITRC20160607-04	Cambridge Institute of International Education (CIIE)	MA	Educational	Yes - Unknown #	Unknown
ITRC20160525-01	Lewis-Palmer School District 38	CO	Educational	Yes - Published #	2,000
ITRC20160524-10	El Paso Independent School District	TX	Educational	Yes - Unknown #	Unknown
ITRC20160517-03	Bingham Junior Hight	MO	Educational	Yes - Unknown #	Unknown
ITRC20160517-02	Poway Unified School District	CA	Educational	Yes - Published #	36,000
ITRC20160516-01	City College of San Francisco	CA	Educational	Yes - Unknown #	Unknown
ITRC20160513-05	Kern County Superintendent of Schools	CA	Educational	Yes - Published #	2,500
ITRC20160513-03	Washington Elementary School District Breach	AZ	Educational	Yes - Unknown #	Unknown
ITRC20160513-02	Kalamazoo College	MI	Educational	Yes - Published #	1,634
ITRC20160512-01	San Mateo Foster City School District	CA	Educational	Yes - Unknown #	Unknown
ITRC20160509-09	Palm Beach County School District	FL	Educational	Yes - Published #	5,800
ITRC20160505-04	California State University Northridge	CA	Educational	Yes - Published #	70,265
ITRC20160503-09	Meeting Street School	RI	Educational	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160503-08	Brunswick School District	ME	Educational	Yes - Unknown #	Unknown
ITRC20160503-07	Allegheny College	PA	Educational	Yes - Unknown #	Unknown
ITRC20160503-01	ProSchools / QuickCert	OR	Educational	Yes - Unknown #	Unknown
ITRC20160502-01	Solano Community College	CA	Educational	Yes - Published #	1,206
ITRC20160429-12	University of the Southwest	NM	Educational	Yes - Unknown #	Unknown
ITRC20160429-06	Bryant & Stratton College	NY	Educational	Yes - Unknown #	Unknown
ITRC20160426-01	Berkeley Public Schools	CA	Educational	Yes - Unknown #	Unknown
ITRC20160425-09	Hutchinson Community College	KS	Educational	Yes - Published #	1,357
ITRC20160425-06	Bowdoin College	ME	Educational	Yes - Published #	275
ITRC20160419-02	Arlington Public Schools	VA	Educational	Yes - Unknown #	Unknown
ITRC20160418-17	Rockhurst University	MO	Educational	Yes - Published #	1,300
ITRC20160418-03	Academy of Art University	NC	Educational	Yes - Unknown #	Unknown
ITRC20160418-02	Olympia School District	WA	Educational	Yes - Published #	2,164
ITRC20160412-01	Stanford University / Equifax W-2Express	CA	Educational	Yes - Published #	600
ITRC20160411-03	Randolph College	VA	Educational	Yes - Published #	100
ITRC20160406-06	Escambia County School System	FL	Educational	Yes - Unknown #	Unknown
ITRC20160405-14	Kentucky State University	KY	Educational	Yes - Published #	1,071
ITRC20160325-01	Tidewater Community College	VA	Educational	Yes - Published #	3,193
ITRC20160321-14	Pulaski County Special School District	AR	Educational	Yes - Published #	2,602
ITRC20160321-09	Sequoia Union High School District	CA	Educational	Yes - Unknown #	Unknown
ITRC20160315-13	Lakes Region Scholarship Foundation	NH	Educational	Yes - Published #	2,047
ITRC20160307-09	Luzerne County Community College	PA	Educational	Yes - Unknown #	Unknown
ITRC20160303-08	Illinois State University	IL	Educational	Yes - Unknown #	Unknown
ITRC20160301-04	Montgomery County School System / WestEd	DC	Educational	Yes - Unknown #	Unknown
ITRC20160226-02	University of California Berkeley	CA	Educational	Yes - Published #	80,000
ITRC20160224-01	Jacksonville State University	AL	Educational	Yes - Unknown #	Unknown
ITRC20160212-03	DC Public School District	DC	Educational	Yes - Published #	12,000
ITRC20160212-02	University of Texas System Administration	TX	Educational	Yes - Published #	794

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20160211-05	Oregon Health & Science University	OR	Educational	Yes - Unknown #	Unknown
ITRC20160208-03	University of Mary Washington	VA	Educational	Yes - Published #	4,100
ITRC20160205-02	Oakmont High School	CA	Educational	Yes - Published #	356
ITRC20160204-02	University of Central Florida	FL	Educational	Yes - Published #	63,000
ITRC20160201-12	Florida International University	FL	Educational	Yes - Unknown #	Unknown
ITRC20160126-08	Lawrence Public Schools	MA	Educational	Yes - Unknown #	Unknown
ITRC20160126-07	Hudson City School District	NY	Educational	Yes - Unknown #	Unknown
ITRC20160122-02	University of Virginia	VA	Educational	Yes - Published #	1,400
ITRC20160120-07	Fitchburg State University	ME	Educational	Yes - Published #	393
ITRC20160120-04	Anna Maria College	ME	Educational	Yes - Published #	1,161
ITRC20160106-01	Southern New Hampshire University	NH	Educational	Yes - Published #	140,000

Totals for Category: Educational

of Breaches: 98 **# of Records: 1,048,342**
% of Breaches: 9.0% **% of Records: 2.9%**

Category: Government/Military

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20161231-01	Pentagon / Potomac Healthcare Solutions	VA	Government/Military	Yes - Unknown #	Unknown
ITRC20161229-13	Forsyth County Tax Commission	GA	Government/Military	Yes - Published #	19,793
ITRC20161229-04	Department of Health and Human Services / New Ham	NH	Government/Military	Yes - Published #	15,000
ITRC20161229-02	Nevada Division of Public and Behavioral Health	NV	Government/Military	Yes - Published #	11,700
ITRC20161219-08	Pentagon	DC	Government/Military	Yes - Published #	3,500
ITRC20161219-01	County of Los Angeles	CA	Government/Military	Yes - Published #	749,017
ITRC20161209-08	Henry County	GA	Government/Military	Yes - Published #	17,841
ITRC20161129-05	Pinellas County Board of County Commissioners	FL	Government/Military	Yes - Published #	2,800
ITRC20161128-20	City of Plummer	ID	Government/Military	Yes - Unknown #	Unknown
ITRC20161128-05	US Navy / Hewlett Packard Enterprise Services	DC	Government/Military	Yes - Published #	134,386
ITRC20161128-02	CDCR - Folsom State Prison	CA	Government/Military	Yes - Unknown #	Unknown
ITRC20161121-08	Internal Revenue Service	DC	Government/Military	Yes - Published #	8,031
ITRC20161121-05	US Department of Housing and Urban Development	DC	Government/Military	Yes - Published #	600,000

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161109-02	VA Eastern Colorado Health Care System	CO	Government/Military	Yes - Published #	2,130
ITRC20161101-01	City of Duluth	MN	Government/Military	Yes - Unknown #	Unknown
ITRC20161031-05	Office of the Comptroller of the Currency	DC	Government/Military	Yes - Published #	10,000
ITRC20161025-03	City of Middletown	NY	Government/Military	Yes - Unknown #	Unknown
ITRC20161013-14	VA Department of Veterans Services / McGuire VA Med	VA	Government/Military	Yes - Published #	5,051
ITRC20161004-08	US Public Health Service Commissioned Corps	DC	Government/Military	Yes - Published #	6,600
ITRC20161004-06	Santa Cruz County Health Services Agency	CA	Government/Military	Yes - Published #	25,000
ITRC20160929-06	Mastic Beach	NY	Government/Military	Yes - Published #	488
ITRC20160923-11	Martin Army Community Hospital	GA	Government/Military	Yes - Published #	1,000
ITRC20160922-01	Ventura County Health Care Agency	CA	Government/Military	Yes - Published #	777
ITRC20160920-03	Oconee County	SC	Government/Military	Yes - Published #	230
ITRC20160919-05	Los Angeles County Department of Health Services	CA	Government/Military	Yes - Published #	743
ITRC20160908-03	U.S. Customs and Border Protection	DC	Government/Military	Yes - Published #	5,000
ITRC20160829-07	Arizona Department of Administration	AZ	Government/Military	Yes - Unknown #	Unknown
ITRC20160829-06	Illinois Board of Elections	IL	Government/Military	Yes - Unknown #	Unknown
ITRC20160829-01	Sacramento County	CA	Government/Military	Yes - Unknown #	Unknown
ITRC20160824-08	Idaho Department of Fish and Game / Active Network	ID	Government/Military	Yes - Published #	788,064
ITRC20160824-07	Oregon Department of Fish and Wildlife / Active Network	OR	Government/Military	Yes - Published #	1,195,204
ITRC20160824-06	Kentucky Department of Fish & Wildlife	KY	Government/Military	Yes - Published #	2,126,449
ITRC20160824-05	Washington Department of Fishing & Wildlife / Active	WA	Government/Military	Yes - Published #	2,435,452
ITRC20160817-01	Nevada Department of Transportation	NV	Government/Military	Yes - Unknown #	Unknown
ITRC20160815-11	County of Anderson	TN	Government/Military	Yes - Published #	1,800
ITRC20160815-09	Department of State Health Services	TX	Government/Military	Yes - Published #	1,500
ITRC20160810-02	FDIC #2	DC	Government/Military	Yes - Published #	30,000
ITRC20160727-02	U.S. Postal Service	CA	Government/Military	Yes - Published #	6,240
ITRC20160719-16	New Hampshire Office of Professional Licensure and	NH	Government/Military	Yes - Unknown #	Unknown
ITRC20160719-11	Montana Department of Public Health and Human Serv	MT	Government/Military	Yes - Published #	185
ITRC20160719-10	Retirement Systems of Alabama	AL	Government/Military	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160712-01	Pennsylvania Department of Revenue	PA	Government/Military	Yes - Published #	865
ITRC20160711-01	California Department of Corrections and Rehabilitatio	CA	Government/Military	Yes - Unknown #	Unknown
ITRC20160624-02	Texas Health and Human Resources Commission	TX	Government/Military	Yes - Published #	600
ITRC20160615-01	Vermont Department of Fish and Wildlife	VT	Government/Military	Yes - Unknown #	Unknown
ITRC20160614-11	Washington State Liquor and Cannabis Board	WA	Government/Military	Yes - Unknown #	Unknown
ITRC20160614-10	Town of Saugus - Lawsuit Discovery	MA	Government/Military	Yes - Published #	1,200
ITRC20160614-09	Virginia's State Corporation Commission	VA	Government/Military	Yes - Unknown #	Unknown
ITRC20160614-07	Sutter County Superior Courthouse	CA	Government/Military	Yes - Unknown #	Unknown
ITRC20160614-05	Kern County Mental Health Department	CA	Government/Military	Yes - Published #	1,212
ITRC20160601-09	Washington DC VA Medical Center	DC	Government/Military	Yes - Published #	1,062
ITRC20160531-05	Department of Agriculture	OH	Government/Military	Yes - Unknown #	Unknown
ITRC20160524-04	San Juan County	NM	Government/Military	Yes - Published #	12,500
ITRC20160516-02	California Correctional Health Care Services	CA	Government/Military	Yes - Published #	400,000
ITRC20160510-10	City of Houston	TX	Government/Military	Yes - Unknown #	Unknown
ITRC20160509-08	FDIC #1	DC	Government/Military	Yes - Published #	40,354
ITRC20160509-07	Ohio Department of Mental Health and Addiction Servi	OH	Government/Military	Yes - Published #	59,000
ITRC20160506-01	Colorado Department of Transportation	CO	Government/Military	Yes - Unknown #	Unknown
ITRC20160421-03	Florida Department of Health	FL	Government/Military	Yes - Published #	1,076
ITRC20160418-05	Town of Essex	VT	Government/Military	Yes - Published #	262
ITRC20160415-01	City of Baltimore	MD	Government/Military	Yes - Unknown #	Unknown
ITRC20160411-05	Federal Deposit Insurance Corp. (FDIC)	DC	Government/Military	Yes - Published #	44,000
ITRC20160411-04	Department of Health - Palm Beach County	FL	Government/Military	Yes - Published #	1,000
ITRC20160411-02	Office of Child Support Enforcement	WA	Government/Military	Yes - Published #	5,000,000
ITRC20160307-05	Department of Human Services - Iowa	IA	Government/Military	Yes - Published #	425
ITRC20160218-03	IRS	DC	Government/Military	Yes - Published #	101,000
ITRC20160216-05	Dallas County	TX	Government/Military	Yes - Unknown #	Unknown
ITRC20160209-01	Department of Homeland Security / FBI	DC	Government/Military	Yes - Unknown #	Unknown
ITRC20160205-03	Department of Human Resource Management	VA	Government/Military	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160126-09	Vermont State Employees	VT	Government/Military	Yes - Unknown #	Unknown
ITRC20160121-01	County of San Diego	CA	Government/Military	Yes - Published #	620
ITRC20160120-06	Town of Amherst	MA	Government/Military	Yes - Published #	414

Totals for Category: Government/Military

of Breaches: 72 # of Records: 13,869,571
% of Breaches: 6.6% % of Records: 37.9%

Category: Medical/Healthcare

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20161231-26	Great Falls Clinic	MT	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161231-14	Renville County Hospital & Clinics	MN	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161231-12	Medtronic	MN	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161231-05	Washington National Insurance Company	IN	Medical/Healthcare	Yes - Published #	1,458
ITRC20161231-04	Washington Health System	PA	Medical/Healthcare	Yes - Published #	544
ITRC20161231-03	ADVANTAGE Health Solutions	IN	Medical/Healthcare	Yes - Published #	2,387
ITRC20161229-22	Upper Connecticut Valley Hospital	NH	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161229-16	Providence Health & Services	WA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161229-09	Brandywine Pediatrics. P.A.	DE	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161229-08	Atmore Community Hospital / Infirmary Health	AL	Medical/Healthcare	Yes - Published #	1,000
ITRC20161229-01	Desert Care Family and Sports Medicine	AZ	Medical/Healthcare	Yes - Published #	500
ITRC20161222-07	Southcentral Foundation	AK	Medical/Healthcare	Yes - Published #	14,719
ITRC20161222-03	Henry County Health Department Home Health and Ho	OH	Medical/Healthcare	Yes - Published #	500
ITRC20161222-02	Fairbanks Hospital	IN	Medical/Healthcare	Yes - Published #	12,994
ITRC20161221-04	Kaiser Permanente	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161221-02	Community Health Plan of Washington	WA	Medical/Healthcare	Yes - Published #	381,534
ITRC20161220-01	4D Sound Diagnostics	TX	Medical/Healthcare	Yes - Published #	1,000
ITRC20161216-04	Oak Cliff Orthopaedic Associates	TX	Medical/Healthcare	Yes - Published #	1,057
ITRC20161215-06	Office of Dr. Melissa D. Selke	MD	Medical/Healthcare	Yes - Published #	4,277
ITRC20161215-04	Office of Charles Stamitoles	FL	Medical/Healthcare	Yes - Published #	5,600
ITRC20161215-03	CHI Franciscan Health Hospice - Tacoma	WA	Medical/Healthcare	Yes - Published #	12,413

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161215-02	Appalachian Gastroenterology, P.A.	NC	Medical/Healthcare	Yes - Published #	11,000
ITRC20161213-01	Quest Diagnostics	NJ	Medical/Healthcare	Yes - Published #	34,055
ITRC20161212-11	PhyMed	TN	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161209-05	Young Adult Institute, Inc.	NY	Medical/Healthcare	Yes - Published #	913
ITRC20161209-04	UnitedHealth Group Single Affiliated Covered Entity #2	MN	Medical/Healthcare	Yes - Published #	1,408
ITRC20161209-03	Preventice Services, LLC	TX	Medical/Healthcare	Yes - Published #	6,800
ITRC20161209-02	CVS Health	RI	Medical/Healthcare	Yes - Published #	626
ITRC20161209-01	Managed Health Services #2	IN	Medical/Healthcare	Yes - Published #	5,500
ITRC20161208-01	East Valley Community Health Center	CA	Medical/Healthcare	Yes - Published #	65,000
ITRC20161206-03	Cleveland Clinic Akron General / Ambucor	OH	Medical/Healthcare	Yes - Published #	730
ITRC20161206-02	New Mexico Heart Institute / Ambucor	NM	Medical/Healthcare	Yes - Published #	4,185
ITRC20161206-01	Glendale Adventist Medical Center / White Memorial M	CA	Medical/Healthcare	Yes - Published #	528
ITRC20161205-09	Vision Care Florida	FL	Medical/Healthcare	Yes - Published #	7,500
ITRC20161205-08	OptumHealth New Mexico	MN	Medical/Healthcare	Yes - Published #	2,006
ITRC20161205-07	Louisiana Health Cooperative, Inc.	LA	Medical/Healthcare	Yes - Published #	8,000
ITRC20161205-06	Sagewood / LCS Westminster Partnership	AZ	Medical/Healthcare	Yes - Published #	863
ITRC20161205-05	Camas Center Clinic / Kalispel Tribe of Indians	WA	Medical/Healthcare	Yes - Published #	504
ITRC20161205-04	Berkshire Medical Center / Ambucor	MA	Medical/Healthcare	Yes - Published #	1,745
ITRC20161205-03	Akron General Medical Center	OH	Medical/Healthcare	Yes - Published #	730
ITRC20161205-02	Group Health Incorporated	NY	Medical/Healthcare	Yes - Published #	81,112
ITRC20161129-06	Consultants in Neurological Surgery, LLP	FL	Medical/Healthcare	Yes - Published #	800
ITRC20161129-04	Lister Healthcare	AL	Medical/Healthcare	Yes - Published #	1,349
ITRC20161129-03	North Texas Heart Center, P.A.	TX	Medical/Healthcare	Yes - Published #	4,210
ITRC20161129-02	Darlington	GA	Medical/Healthcare	Yes - Published #	600
ITRC20161128-06	Aetna Signature Administrators	CT	Medical/Healthcare	Yes - Published #	18,854
ITRC20161128-04	Vascular Surgical Associates	GA	Medical/Healthcare	Yes - Published #	36,496
ITRC20161122-07	Conemaugh Health System / Ambucor	PA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161122-06	Stony Brook Heart Institute / University Faculty Practic	NY	Medical/Healthcare	Yes - Unknown #	Unknown

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161122-05	Northwell Health / Lenox Hill Heart and Vascular Instit	NY	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161122-04	Main Line HealthCare / Ambucor	PA	Medical/Healthcare	Yes - Published #	4,500
ITRC20161122-03	Wentworth-Douglass Hospital / Ambucor	NH	Medical/Healthcare	Yes - Published #	775
ITRC20161121-07	Briar Hill Management	MS	Medical/Healthcare	Yes - Published #	2,000
ITRC20161121-06	Biomechanics LLC / Rehab Billing Solutions	AZ	Medical/Healthcare	Yes - Published #	1,049
ITRC20161121-01	Eye Institute of Marin (Marin Medical Practice Concept	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161118-11	George Gillian, DDS	AR	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161118-09	Lebanon Cardiology Associates, PC / Ambucor	PA	Medical/Healthcare	Yes - Published #	537
ITRC20161118-08	Horizon Blue Cross Blue Shield of New Jersey / Comm	NJ	Medical/Healthcare	Yes - Published #	170,000
ITRC20161118-07	Emblem Health	NY	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161118-06	KinetoRehab Physical Therapy	NY	Medical/Healthcare	Yes - Published #	665
ITRC20161118-05	Wal-Mart Stores, Inc.	AR	Medical/Healthcare	Yes - Published #	771
ITRC20161118-01	Luque Chiropractic, Inc. / Watsonville Chiropractic, Inc	CA	Medical/Healthcare	Yes - Published #	1,341
ITRC20161115-11	Indiana Health Coverage Program / HP Enterprise Serv	TX	Medical/Healthcare	Yes - Published #	1,235
ITRC20161115-10	HeartCare Consultants	FL	Medical/Healthcare	Yes - Published #	16,000
ITRC20161115-09	Harrisonburg OB GYN Associates, P.C.	VA	Medical/Healthcare	Yes - Published #	800
ITRC20161115-08	Kaiser Permanente Health Plan, Inc. (Northern Californ	CA	Medical/Healthcare	Yes - Published #	4,432
ITRC20161115-07	Kaiser Permanente Health Plan, Inc. (Southern Californ	CA	Medical/Healthcare	Yes - Published #	3,044
ITRC20161115-06	Austin Pulmonary Consultants	TX	Medical/Healthcare	Yes - Published #	889
ITRC20161115-05	Best Health Physical Therapy, LLC / Rehab Billing Solu	CT	Medical/Healthcare	Yes - Published #	1,100
ITRC20161114-02	Broward Health Imperial Point	FL	Medical/Healthcare	Yes - Published #	126
ITRC20161114-01	Seguin Dermatology	TX	Medical/Healthcare	Yes - Published #	29,969
ITRC20161108-01	Kaiser Foundation Health Plan of the Northwest	OR	Medical/Healthcare	Yes - Published #	544
ITRC20161107-03	Singh and Arora Oncology Hematology, PC	MI	Medical/Healthcare	Yes - Published #	16,000
ITRC20161107-02	MGA Home Healthcare	AZ	Medical/Healthcare	Yes - Published #	3,119
ITRC20161107-01	Four Star Drug of Bethany, Inc.	NE	Medical/Healthcare	Yes - Published #	647
ITRC20161101-05	You and Your Health Family Care, Inc.	FL	Medical/Healthcare	Yes - Published #	3,000
ITRC20161101-04	Office of Dr. Dennis T. Myers, DDS, PA	MO	Medical/Healthcare	Yes - Published #	3,364

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161101-03	Anthem	IN	Medical/Healthcare	Yes - Published #	3,525
ITRC20161031-09	Symphony Health Solutions Corporation	PA	Medical/Healthcare	Yes - Published #	365
ITRC20161031-08	AxoGen	FL	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161031-07	Anthelio Healthcare Solutions, Inc.	TX	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161031-02	Office of Anne M. Cummings, MD, FACP / Marin Medic	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161027-01	Finley Center for Acupuncture and Naturopathic Medic	NV	Medical/Healthcare	Yes - Published #	3,000
ITRC20161026-05	Greater Florida Anesthesiologists	FL	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161025-01	Silver Creek Physical Therapy Entities	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161024-05	Remedi SeniorCare	MD	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161024-04	BioTime, Inc.	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161021-07	Seattle Indian Health Board	WA	Medical/Healthcare	Yes - Published #	793
ITRC20161021-06	Baystate Health	MA	Medical/Healthcare	Yes - Published #	13,112
ITRC20161021-05	Florida Hospital Medical Group	FL	Medical/Healthcare	Yes - Published #	6,786
ITRC20161021-03	Health Access Network / Lincoln Medical Center	ME	Medical/Healthcare	Yes - Published #	17,000
ITRC20161019-03	Genesis Physical Therapy	CA	Medical/Healthcare	Yes - Published #	2,245
ITRC20161019-01	Mercy Hospital and Medical Center	IL	Medical/Healthcare	Yes - Published #	547
ITRC20161018-08	Office of Curtis F. Robinson, MD, Inc. / Marin Medical	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161018-07	Integrity Transitional Hospital	TX	Medical/Healthcare	Yes - Published #	29,514
ITRC20161018-06	CalOptima #2	CA	Medical/Healthcare	Yes - Published #	56,000
ITRC20161018-05	Fred's Stores of Tennessee	TN	Medical/Healthcare	Yes - Published #	9,624
ITRC20161018-04	Warren Clinic	OK	Medical/Healthcare	Yes - Published #	2,938
ITRC20161018-03	Rainbow Children's Clinic	TX	Medical/Healthcare	Yes - Published #	33,698
ITRC20161018-02	Peabody Retirement Community	IN	Medical/Healthcare	Yes - Published #	1,466
ITRC20161013-20	Office of Francisco Jaume, D.O.	AZ	Medical/Healthcare	Yes - Published #	14,236
ITRC20161013-19	Baxter Regional Medical Center - Home Health Facility	AR	Medical/Healthcare	Yes - Published #	2,124
ITRC20161013-18	Baxter Healthcare	IL	Medical/Healthcare	Yes - Published #	992
ITRC20161013-17	Apria Healthcare	CA	Medical/Healthcare	Yes - Published #	1,987
ITRC20161013-16	Marin Healthcare District / Marin Medical Practices Co	CA	Medical/Healthcare	Yes - Published #	2,292

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20161013-15	Thomasville Eye Center	GA	Medical/Healthcare	Yes - Published #	10,891
ITRC20161013-13	Peachtree Orthopedics	GA	Medical/Healthcare	Yes - Published #	531,000
ITRC20161013-12	University of Wisconsin HealthCenter	WI	Medical/Healthcare	Yes - Published #	6,923
ITRC20161013-11	Northwest Community Hospital / R-C Healthcare Mana	IL	Medical/Healthcare	Yes - Published #	540
ITRC20161013-08	Group Health Cooperative	WA	Medical/Healthcare	Yes - Published #	668
ITRC20161013-07	Vermont Health Connect / WEX / Samanage	CT	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20161013-01	Office of Hal Meadows, MD	CA	Medical/Healthcare	Yes - Published #	6,000
ITRC20161004-11	Prima Medical Foundation / Marin Medical Practices C	CA	Medical/Healthcare	Yes - Published #	Unknown
ITRC20161004-09	Urgent Care Clinic of Oxford	MS	Medical/Healthcare	Yes - Published #	64,000
ITRC20161004-07	Willow Bend Dental	TX	Medical/Healthcare	Yes - Published #	625
ITRC20161004-05	San Juan Oncology Associates	NM	Medical/Healthcare	Yes - Published #	500
ITRC20161004-04	McLaren Greater Lansing Cardiovascular Group	MI	Medical/Healthcare	Yes - Published #	1,000
ITRC20161004-03	Jennie Stuart Medical Center	KY	Medical/Healthcare	Yes - Published #	1,500
ITRC20161004-02	Heritage Medical Partners	SC	Medical/Healthcare	Yes - Published #	812
ITRC20160929-04	New Jersey Spine Center	NJ	Medical/Healthcare	Yes - Published #	28,308
ITRC20160929-02	Vermont Health Connect #1	VT	Medical/Healthcare	Yes - Published #	700
ITRC20160927-01	Public Education Employees' Health Insurance Plan	AL	Medical/Healthcare	Yes - Published #	1,349
ITRC20160923-09	Asante Health System	OR	Medical/Healthcare	Yes - Published #	2,400
ITRC20160923-08	Codman Square Health Center	MA	Medical/Healthcare	Yes - Published #	3,840
ITRC20160923-07	Office of Hal Meadows, M.D.	CA	Medical/Healthcare	Yes - Published #	6,000
ITRC20160923-05	Napa Valley Dentistry	CA	Medical/Healthcare	Yes - Published #	4,262
ITRC20160923-01	USC Keck Medical Center	CA	Medical/Healthcare	Yes - Published #	16,000
ITRC20160922-02	KidsPeace	PA	Medical/Healthcare	Yes - Published #	1,456
ITRC20160920-01	Saint Francis Health System	OK	Medical/Healthcare	Yes - Published #	6,000
ITRC20160919-17	Decatur Health Systems	KS	Medical/Healthcare	Yes - Published #	707
ITRC20160919-16	King of Prussia Dental Associates	PA	Medical/Healthcare	Yes - Published #	16,228
ITRC20160919-09	Office of Pratap S. Kurra, M.D.	CA	Medical/Healthcare	Yes - Published #	2,029
ITRC20160919-07	St. Elizabeth Physicians (Summit Medical Group)	KY	Medical/Healthcare	Yes - Published #	674

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160919-06	CalOptima #1	CA	Medical/Healthcare	Yes - Published #	1,000
ITRC20160919-04	Geisinger Health Plan	PA	Medical/Healthcare	Yes - Published #	2,814
ITRC20160919-03	University Gastroenterology, Inc.	RI	Medical/Healthcare	Yes - Published #	15,478
ITRC20160919-02	U.S. Healthworks	CA	Medical/Healthcare	Yes - Published #	1,400
ITRC20160919-01	CHI Franciscan Health / St. Clare Hospital / St. Joseph	WA	Medical/Healthcare	Yes - Published #	2,818
ITRC20160915-01	Yuba Sutter Medical Clinic	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160908-05	Southwest Portland Dental / Patterson Dental Supply, I	OR	Medical/Healthcare	Yes - Published #	1,980
ITRC20160908-02	Children's Mercy Hospital	MO	Medical/Healthcare	Yes - Published #	238
ITRC20160908-01	Burrell Behavioral Health	MO	Medical/Healthcare	Yes - Published #	7,748
ITRC20160907-05	Village of Oak Park	IL	Medical/Healthcare	Yes - Published #	688
ITRC20160907-04	Planned Parenthood of Greater Washington and North	WA	Medical/Healthcare	Yes - Published #	10,700
ITRC20160907-02	CHI Franciscan Healthcare Highline Medical Center / R	WA	Medical/Healthcare	Yes - Published #	18,399
ITRC20160907-01	Cardiology Associates	MD	Medical/Healthcare	Yes - Published #	907
ITRC20160906-02	Medical College of Wisconsin	WI	Medical/Healthcare	Yes - Published #	3,179
ITRC20160830-04	Office of Dr. Richard Boehm	TN	Medical/Healthcare	Yes - Published #	500
ITRC20160830-02	Appalachian Regional Healthcare	NC	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160830-01	USC Medical Center	CA	Medical/Healthcare	Yes - Published #	700
ITRC20160829-05	Phoenix Dental Care	TN	Medical/Healthcare	Yes - Published #	6,441
ITRC20160825-03	DXE Medical	TN	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160824-16	Orleans Medical Clinic	IN	Medical/Healthcare	Yes - Published #	6,890
ITRC20160824-14	Center for Neurosurgical and Spinal Disorders	LA	Medical/Healthcare	Yes - Published #	1,134
ITRC20160824-13	Rotech Healthcare	FL	Medical/Healthcare	Yes - Published #	957
ITRC20160824-11	Eastern Carolina Cardiovascular / Outer Banks Hospita	NC	Medical/Healthcare	Yes - Published #	1,000
ITRC20160824-09	Scan Health Plan	CA	Medical/Healthcare	Yes - Published #	87,069
ITRC20160824-03	Dominican Hospital	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160816-02	Neurology Physicians LLC	MD	Medical/Healthcare	Yes - Published #	4,831
ITRC20160816-01	Autism Home Support Services	IL	Medical/Healthcare	Yes - Published #	533
ITRC20160815-10	EXOS (Athletes' Performance)	AZ	Medical/Healthcare	Yes - Published #	854

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC ID	Organization	State	Industry	Published	Count
ITRC20160815-07	Office of John E. Gonzalez, DDS	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160815-06	Valley Anesthesiology and Pain Consultants	AZ	Medical/Healthcare	Yes - Published #	882,590
ITRC20160815-05	Bon Secours Health Systems / R-C Healthcare Manage	MD	Medical/Healthcare	Yes - Published #	655,203
ITRC20160815-02	Office of Brian Halevie-Goldman, MD	CA	Medical/Healthcare	Yes - Published #	2,000
ITRC20160809-06	Carle Foundation Hospital	IL	Medical/Healthcare	Yes - Published #	1,185
ITRC20160809-04	Professional Dermatology Care, PC	VA	Medical/Healthcare	Yes - Published #	13,237
ITRC20160808-02	Newkirk Products	NY	Medical/Healthcare	Yes - Published #	3,466,120
ITRC20160805-01	Banner Health	AZ	Medical/Healthcare	Yes - Published #	3,623,140
ITRC20160802-26	inVentiv Health	MA	Medical/Healthcare	Yes - Published #	14,604
ITRC20160802-23	Office of Ceaton C. Falgiano	NY	Medical/Healthcare	Yes - Published #	650
ITRC20160802-22	Heart Center of Southern Maryland, LLP	MD	Medical/Healthcare	Yes - Published #	1,350
ITRC20160802-21	Cefalu Eye-Tech of Green, Inc.	OH	Medical/Healthcare	Yes - Published #	850
ITRC20160802-20	Sunshine State Health Plan, Inc.	FL	Medical/Healthcare	Yes - Published #	1,479
ITRC20160802-19	Caring for Women, P.A.	TX	Medical/Healthcare	Yes - Published #	697
ITRC20160802-18	Greenville Health System (Carolina Cardiology) / Ambu	DE	Medical/Healthcare	Yes - Published #	2,500
ITRC20160802-17	Premier Family Care / Mario M. Gross M.D.	TX	Medical/Healthcare	Yes - Published #	1,326
ITRC20160802-16	StarCare Specialty Health System	TX	Medical/Healthcare	Yes - Published #	2,900
ITRC20160802-14	Midwest Orthopedics Group	MO	Medical/Healthcare	Yes - Published #	29,153
ITRC20160802-13	Athens Orthopedic Clinic	GA	Medical/Healthcare	Yes - Published #	201,000
ITRC20160802-12	Memorial Hermann	TX	Medical/Healthcare	Yes - Published #	12,061
ITRC20160802-11	Lifewellness Institute / Bizmatics	CA	Medical/Healthcare	Yes - Published #	2,473
ITRC20160802-10	Jefferson Medical Associates	MS	Medical/Healthcare	Yes - Published #	10,401
ITRC20160802-09	Prosthetic & Orthotic Care	MO	Medical/Healthcare	Yes - Published #	23,015
ITRC20160802-08	Crozer-Keystone Health System / Center for Minimally I	PA	Medical/Healthcare	Yes - Published #	900
ITRC20160802-06	University of Arkansas for Medical Sciences	AR	Medical/Healthcare	Yes - Published #	42
ITRC20160802-04	Access Health Care Physicians	FL	Medical/Healthcare	Yes - Published #	2,500
ITRC20160802-03	Blaine Chiropractic Center	MN	Medical/Healthcare	Yes - Published #	1,945
ITRC20160802-02	American Family Care	AL	Medical/Healthcare	Yes - Published #	7,200

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160802-01	Central Ohio Urology Group	OH	Medical/Healthcare	Yes - Published #	300,000
ITRC20160722-02	College Hill Health Center	WY	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160722-01	Sunbury Plaza Dental	OH	Medical/Healthcare	Yes - Published #	7,784
ITRC20160719-14	Health Incent, LLC	TN	Medical/Healthcare	Yes - Published #	1,100
ITRC20160719-13	Lasair Aesthetic Health, P.C.	CO	Medical/Healthcare	Yes - Published #	1,835
ITRC20160719-09	Providence Medical Group - Gateway Clinics	OR	Medical/Healthcare	Yes - Published #	5,978
ITRC20160719-02	Kaiser Permanente Northern California	CA	Medical/Healthcare	Yes - Published #	1,136
ITRC20160712-09	Arkansas Spine and Pain / Bizmatics	AR	Medical/Healthcare	Yes - Published #	17,100
ITRC20160712-08	My Pediatrician, PA / Bizmatics	FL	Medical/Healthcare	Yes - Published #	2,500
ITRC20160712-07	North Ottawa Medical Group / Bizmatics	MI	Medical/Healthcare	Yes - Published #	22,000
ITRC20160712-06	Laser & Dermatologic Surgery Center	MO	Medical/Healthcare	Yes - Published #	31,000
ITRC20160712-05	Midland Women's Clinic / Mario M. Gross, M.D.	TX	Medical/Healthcare	Yes - Published #	717
ITRC20160712-04	Uncommon Care, P.A. / Bizmatics	NC	Medical/Healthcare	Yes - Published #	13,674
ITRC20160712-02	Ambulatory Surgery Center at St. Mary	PA	Medical/Healthcare	Yes - Published #	13,000
ITRC20160711-04	Midland Memorial Hospital / Mario M. Gross, M.D.	TX	Medical/Healthcare	Yes - Published #	1,468
ITRC20160711-02	PruittHealth Hospice - Beaufort	GA	Medical/Healthcare	Yes - Published #	1,437
ITRC20160705-07	Allergy, Asthma & Immunology of the Rockies	CO	Medical/Healthcare	Yes - Published #	6,851
ITRC20160705-06	Office of Linda J. White, DDS, PC	VA	Medical/Healthcare	Yes - Published #	2,000
ITRC20160705-02	Massachusetts General Hospital / Patterson Dental Su	MA	Medical/Healthcare	Yes - Published #	4,293
ITRC20160705-01	Planned Parenthood of the Heartland	IA	Medical/Healthcare	Yes - Published #	2,506
ITRC20160628-03	Riverside Health System	VA	Medical/Healthcare	Yes - Published #	578
ITRC20160627-01	Dignity Health / Mercy Medical Center Redding	CA	Medical/Healthcare	Yes - Published #	520
ITRC20160624-01	Saints Mary and Elizabeth Hospital	KY	Medical/Healthcare	Yes - Published #	1,682
ITRC20160621-02	Massachusetts Eye and Ear Infirmary, Inc.	MA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160620-08	Vein Doctor / Bizmatics	MO	Medical/Healthcare	Yes - Published #	3,000
ITRC20160620-07	Grace Primary Care, PC / Bizmatics	TN	Medical/Healthcare	Yes - Published #	6,853
ITRC20160620-04	Wal-Mart	AR	Medical/Healthcare	Yes - Published #	27,393
ITRC20160620-03	ENT and Allergy Center / BizMatics	AR	Medical/Healthcare	Yes - Published #	16,200

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160620-02	Hamilton General Hospital	TX	Medical/Healthcare	Yes - Published #	397
ITRC20160614-14	ARIAD Pharmaceuticals	MA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160614-12	Office of Allen Dell, PA	FL	Medical/Healthcare	Yes - Published #	2,500
ITRC20160614-06	Vincent Vein Center Grand Junction / Bizmatics	CO	Medical/Healthcare	Yes - Published #	2,250
ITRC20160614-01	Momentum for Mental Health	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160607-11	Northwest Oncology & Hematology, S.C.	IL	Medical/Healthcare	Yes - Published #	1,625
ITRC20160607-10	Edwin Shaw Rehabilitation	OH	Medical/Healthcare	Yes - Published #	975
ITRC20160607-09	AFLAC	GA	Medical/Healthcare	Yes - Published #	930
ITRC20160607-08	Orchid MPS Holdings, LLC / Welfare Benefit Plan	MI	Medical/Healthcare	Yes - Published #	771
ITRC20160607-03	University of New Mexico Hospital	NM	Medical/Healthcare	Yes - Published #	2,827
ITRC20160607-02	Loyola University Medical Center	IL	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160606-01	ProMedica / Herrick Hospital	MI	Medical/Healthcare	Yes - Published #	3,472
ITRC20160601-10	Keystone Rural Health Consortia	PA	Medical/Healthcare	Yes - Published #	800
ITRC20160601-08	California Health & Longevity Institute / Bizmatics	CA	Medical/Healthcare	Yes - Published #	4,386
ITRC20160601-07	Integrated Health Solutions / Bizmatics	PA	Medical/Healthcare	Yes - Published #	19,776
ITRC20160601-03	Stamford Podiatry Group / Bizmatics	CT	Medical/Healthcare	Yes - Published #	40,491
ITRC20160601-01	Verity Health System	OR	Medical/Healthcare	Yes - Published #	7,604
ITRC20160531-08	Kline Galland / Caroline Kline Galland Home / Galland	WA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160531-04	Emergency Medicine Associates (Carondelet)	AZ	Medical/Healthcare	Yes - Published #	1,067
ITRC20160531-03	Tallahassee Memorial Healthcare, Inc.	FL	Medical/Healthcare	Yes - Published #	505
ITRC20160531-02	Surgical Care Affiliates	AL	Medical/Healthcare	Yes - Published #	9,009
ITRC20160531-01	Associates in EyeCare, PSC	KY	Medical/Healthcare	Yes - Published #	971
ITRC20160524-18	UnitedHealth Group Single Affiliated Covered Entity (S	MN	Medical/Healthcare	Yes - Published #	5,330
ITRC20160524-17	Southeast Eye Institute, PA dba Associates of Pinellas	FL	Medical/Healthcare	Yes - Published #	87,314
ITRC20160524-16	Lafayette Pain Care PC / Bizmatics	IN	Medical/Healthcare	Yes - Published #	7,500
ITRC20160524-15	Family Medicine of Weston / Bizmatics	FL	Medical/Healthcare	Yes - Published #	500
ITRC20160524-14	Employee Benefits Division	AR	Medical/Healthcare	Yes - Published #	2,602
ITRC20160524-13	Coordinated Health Mutual, Inc.	OH	Medical/Healthcare	Yes - Published #	591

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160524-11	Comanche County Memorial Hospital / Memorial Medic	OK	Medical/Healthcare	Yes - Published #	2,199
ITRC20160524-05	Berkeley Endocrine Clinic	CA	Medical/Healthcare	Yes - Published #	1,370
ITRC20160524-03	Complete Chiropractic and Bodywork Therapies	MI	Medical/Healthcare	Yes - Published #	4,082
ITRC20160517-01	Zocdoc, Inc.	NY	Medical/Healthcare	Yes - Published #	17,000
ITRC20160516-05	Imperial Valley Family Care Medical Group	CA	Medical/Healthcare	Yes - Published #	649
ITRC20160516-04	PruittHealth Home Health - Low Country	SC	Medical/Healthcare	Yes - Published #	1,500
ITRC20160512-06	Medical Colleagues of Texas	TX	Medical/Healthcare	Yes - Published #	68,631
ITRC20160512-05	Children's National Health System / Ascend Healthcare	DC	Medical/Healthcare	Yes - Published #	4,107
ITRC20160512-04	UnityPoint Health / Allen Hospital	IA	Medical/Healthcare	Yes - Published #	1,620
ITRC20160512-03	Office of Mark Anthony Quintero, MD, LLC / Bizmatic	FL	Medical/Healthcare	Yes - Published #	650
ITRC20160512-02	Florida Medical Clinic, PA / Greenway Health	FL	Medical/Healthcare	Yes - Published #	1,000
ITRC20160510-09	National Counseling Group	VA	Medical/Healthcare	Yes - Published #	23,000
ITRC20160510-06	Family & Children's Services of Mid Michigan, Inc.	MI	Medical/Healthcare	Yes - Published #	981
ITRC20160510-05	Northstar Healthcare Acquisitions LLC / Equalize Reve	TX	Medical/Healthcare	Yes - Published #	19,898
ITRC20160510-04	Managed Health Services	IN	Medical/Healthcare	Yes - Published #	610
ITRC20160510-03	Mayfield Clinic of Cincinnati	OH	Medical/Healthcare	Yes - Published #	23,341
ITRC20160505-05	Saint Agnes Medical Center	CA	Medical/Healthcare	Yes - Published #	2,812
ITRC20160503-16	Smith & Nephew PLC (Blue Belt Technologies)	MN	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160503-06	Florida Hospital Medical Group	FL	Medical/Healthcare	Yes - Published #	1,906
ITRC20160503-03	EqualizeRCM Services	TX	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160429-08	Vail Valley	CO	Medical/Healthcare	Yes - Published #	3,118
ITRC20160426-12	Seven Hills Foundation	MA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160426-10	Mountain Park Health Center	AZ	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160426-02	Akron General Edwin Shaw Rehabilitation	OH	Medical/Healthcare	Yes - Published #	975
ITRC20160425-05	Kaiser Permanente - Inland Empire	CA	Medical/Healthcare	Yes - Published #	2,451
ITRC20160425-03	RMA Medical Centers of Florida	FL	Medical/Healthcare	Yes - Published #	3,906
ITRC20160425-02	Sacred Heart Health System, Inc.	FL	Medical/Healthcare	Yes - Published #	532
ITRC20160425-01	American Fidelity Assurance Company	OK	Medical/Healthcare	Yes - Published #	2,664

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160421-12	Wyoming Medical Center	WY	Medical/Healthcare	Yes - Published #	3,184
ITRC20160421-09	Vibrant Body Wellness	CA	Medical/Healthcare	Yes - Published #	726
ITRC20160421-08	Sisters of Charity of Leavenworth Health System Healt	CO	Medical/Healthcare	Yes - Published #	540
ITRC20160421-07	BioReference Laboratories, Inc.	NJ	Medical/Healthcare	Yes - Published #	3,563
ITRC20160421-06	Target Corporation Health Plan	MN	Medical/Healthcare	Yes - Published #	719
ITRC20160421-04	United Community & Family Services	CT	Medical/Healthcare	Yes - Published #	1,000
ITRC20160421-02	Lake Pulmonary Critical PA	FL	Medical/Healthcare	Yes - Published #	648
ITRC20160420-04	Clinton Health Access Initiative	MA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160420-03	Convey Health Solutions	FL	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160420-01	Pain Treatment Centers of America / Interventional Sur	AR	Medical/Healthcare	Yes - Published #	19,397
ITRC20160419-03	CVS Alabama Pharmacy	AL	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160418-11	Management Health Systems, Inc. dba MedPro Healthc	FL	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160418-07	Atique Orthodontics	TX	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160411-01	OptumRx	MN	Medical/Healthcare	Yes - Published #	6,229
ITRC20160408-03	Einstein Health Network	PA	Medical/Healthcare	Yes - Published #	2,939
ITRC20160406-05	Lindsay House Surgery Center	NY	Medical/Healthcare	Yes - Published #	773
ITRC20160406-04	Excel Plus Home Health, Inc.	TX	Medical/Healthcare	Yes - Published #	524
ITRC20160405-13	Indian Health Service / Norther Navajo Medical Center	NM	Medical/Healthcare	Yes - Published #	7,421
ITRC20160405-12	Kings Daughters Health	IN	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160405-11	Alvarado Hospital Medical Center / Prime Healthcare	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160405-07	IASIS Healthcare	TN	Medical/Healthcare	Yes - Published #	18,273
ITRC20160405-05	Morton Medical Center PLLC	WA	Medical/Healthcare	Yes - Published #	3,000
ITRC20160405-04	Aurora Health Care, Inc.	WI	Medical/Healthcare	Yes - Published #	869
ITRC20160405-03	Pointe Medical Services, Inc.	FL	Medical/Healthcare	Yes - Published #	2,000
ITRC20160405-02	Metropolitan Jewish Health System, Inc.	NY	Medical/Healthcare	Yes - Published #	2,483
ITRC20160404-09	Val Verde Regional Medical Center	TX	Medical/Healthcare	Yes - Published #	2,000
ITRC20160404-08	Cardiology Associates of Jonesboro, Inc.	AR	Medical/Healthcare	Yes - Published #	1,669
ITRC20160404-07	Group Life Hospital and Medical Program	CT	Medical/Healthcare	Yes - Published #	3,000

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160404-06	Ecolab Health and Welfare Benefits Plan	MN	Medical/Healthcare	Yes - Published #	1,550
ITRC20160404-05	Bozeman Health Deaconness Hospital	MT	Medical/Healthcare	Yes - Published #	1,124
ITRC20160404-03	MedStar Health	DC	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160404-02	Blue Chip Dental	MI	Medical/Healthcare	Yes - Published #	2,200
ITRC20160329-07	Northgate Medical	MA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160329-04	Mind Springs Health	CO	Medical/Healthcare	Yes - Published #	2,147
ITRC20160329-03	Walgreen Co.	IL	Medical/Healthcare	Yes - Published #	880
ITRC20160329-02	Office of W. Christopher Bryant DDS	MI	Medical/Healthcare	Yes - Published #	2,200
ITRC20160329-01	Hospital for Special Surgery	NY	Medical/Healthcare	Yes - Published #	647
ITRC20160328-02	Mercy Iowa City / Mercy Clinics	IN	Medical/Healthcare	Yes - Published #	15,625
ITRC20160324-02	Kids Dental Care	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160324-01	JASACare	NY	Medical/Healthcare	Yes - Published #	1,154
ITRC20160323-01	CareCentrix	CT	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160322-06	eClinical Works, LLC	MA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160322-05	Complete Family Foot Care / Bizmatics	NE	Medical/Healthcare	Yes - Published #	5,883
ITRC20160322-04	Illinois Valley Podiatry Group / Bizmatics	IL	Medical/Healthcare	Yes - Published #	26,588
ITRC20160322-03	Grand Street Medical Associates	NY	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160321-05	Lakewood Hills Internal Medicine / Felicia Lewis, MD	TX	Medical/Healthcare	Yes - Published #	1,500
ITRC20160321-04	Locust Fork Pharmacy	AL	Medical/Healthcare	Yes - Published #	5,000
ITRC20160321-03	Virtua Medical Group	NJ	Medical/Healthcare	Yes - Published #	1,654
ITRC20160321-02	Office of Elliot J. Martin Chiropractic, PC	NY	Medical/Healthcare	Yes - Published #	1,200
ITRC20160321-01	Centers Plan for Healthy Living	NY	Medical/Healthcare	Yes - Published #	6,893
ITRC20160315-10	Endologix	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160315-09	University Hospitals Geauga Medical Center	OH	Medical/Healthcare	Yes - Published #	677
ITRC20160315-07	Karmanos Cancer Center	MI	Medical/Healthcare	Yes - Published #	2,808
ITRC20160308-02	Blue Cross Blue Shield - South Carolina	SC	Medical/Healthcare	Yes - Published #	998
ITRC20160308-01	Premier Healthcare	IN	Medical/Healthcare	Yes - Published #	205,748
ITRC20160307-06	City of Hope Hospital	CA	Medical/Healthcare	Yes - Published #	1,024

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160307-04	21st Century Oncology	FL	Medical/Healthcare	Yes - Published #	2,213,597
ITRC20160307-03	Freeport Memorial Hospital	IL	Medical/Healthcare	Yes - Published #	1,349
ITRC20160307-02	Roark's Pharmacy	TN	Medical/Healthcare	Yes - Published #	2,393
ITRC20160307-01	Public Health Trust of Miami-Dade, FL	FL	Medical/Healthcare	Yes - Published #	24,188
ITRC20160303-06	Wal-Mart Stores, Inc. (Pharmacy)	AR	Medical/Healthcare	Yes - Published #	4,800
ITRC20160303-05	Nintendo Health Plan / Premera	WA	Medical/Healthcare	Yes - Published #	6,248
ITRC20160303-04	Main Line Health	PA	Medical/Healthcare	Yes - Published #	11,000
ITRC20160303-03	Eye Institute of Corpus Christi / Dr. Ravi Krishnan	TX	Medical/Healthcare	Yes - Published #	43,961
ITRC20160301-05	FHN Memorial Hospital	IL	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160301-01	BJC Healthcare ACO, LLC	MO	Medical/Healthcare	Yes - Published #	2,393
ITRC20160229-01	Vancouver Radiologists	WA	Medical/Healthcare	Yes - Published #	603
ITRC20160226-04	Valley Hope Association	KS	Medical/Healthcare	Yes - Published #	52,076
ITRC20160225-02	Bay Area Chiropractic Center	OR	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160225-01	York Hospital	ME	Medical/Healthcare	Yes - Published #	1,400
ITRC20160223-02	United Medical / Lincare Inc.	FL	Medical/Healthcare	Yes - Published #	278
ITRC20160223-01	Saint Joseph's Healthcare System	NJ	Medical/Healthcare	Yes - Published #	5,924
ITRC20160222-03	Rite Aid Store #01617	NY	Medical/Healthcare	Yes - Published #	976
ITRC20160222-02	DataStat, Inc.	MI	Medical/Healthcare	Yes - Published #	552
ITRC20160218-02	Shire Human Genetic Therapies	MA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160216-04	Vidant Health	NC	Medical/Healthcare	Yes - Published #	897
ITRC20160216-02	Magnolia Health Corporation	CA	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160211-04	Jackson Health System	FL	Medical/Healthcare	Yes - Published #	24,188
ITRC20160210-01	Washington State Health Authority (HCA) / Medicaid	WA	Medical/Healthcare	Yes - Published #	91,187
ITRC20160209-02	Seim Johnson, LLP	NE	Medical/Healthcare	Yes - Published #	30,972
ITRC20160205-01	Borgess Rheumatology	MI	Medical/Healthcare	Yes - Published #	700
ITRC20160204-01	Medicap Pharmacy	IA	Medical/Healthcare	Yes - Published #	2,300
ITRC20160202-03	Crown Point Health Center	IN	Medical/Healthcare	Yes - Published #	1,854
ITRC20160202-02	Hawaii Medical Service Association	HI	Medical/Healthcare	Yes - Published #	10,179

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

ITRC20160201-11	Louisiana Healthcare Connections	LA	Medical/Healthcare	Yes - Published #	13,086
ITRC20160201-10	Wayne Memorial Hospital	PA	Medical/Healthcare	Yes - Published #	390
ITRC20160201-09	AHRC Nassau	NY	Medical/Healthcare	Yes - Published #	1,200
ITRC20160201-08	G & S Medical Associates, LLC	NJ	Medical/Healthcare	Yes - Published #	3,000
ITRC20160201-07	Livongo Health, Inc.	IL	Medical/Healthcare	Yes - Published #	1,950
ITRC20160201-06	NCH Healthcare System	FL	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160126-06	Centene	MO	Medical/Healthcare	Yes - Published #	950,000
ITRC20160126-04	HealthEquity	UT	Medical/Healthcare	Yes - Unknown #	Unknown
ITRC20160121-02	Elite Imaging	FL	Medical/Healthcare	Yes - Published #	1,457
ITRC20160119-09	WhiteGlove Health	TX	Medical/Healthcare	Yes - Published #	975
ITRC20160119-08	Allina Health	MN	Medical/Healthcare	Yes - Published #	6,195
ITRC20160119-07	Brigham and Women's Hospital	MA	Medical/Healthcare	Yes - Published #	1,009
ITRC20160119-06	New West Health Services	MT	Medical/Healthcare	Yes - Published #	28,209
ITRC20160119-01	Blue Shield of California	CA	Medical/Healthcare	Yes - Published #	20,764
ITRC20160112-02	Oceans Acquisition, Inc.	TX	Medical/Healthcare	Yes - Published #	659
ITRC20160112-01	St. Luke's Cornwall Hospital	NY	Medical/Healthcare	Yes - Published #	29,156
ITRC20160111-01	Pittman Family Dental	OH	Medical/Healthcare	Yes - Published #	8,830
ITRC20160108-03	Fidelis Care	NY	Medical/Healthcare	Yes - Published #	738
ITRC20160108-01	Indiana University Health Arnett Hospital	IN	Medical/Healthcare	Yes - Published #	29,324

Totals for Category: Medical/Healthcare

of Breaches: 376 # of Records: 15,942,053
% of Breaches: 34.4 %of Records: 43.6%

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Totals for All Categories : # of Breaches: 1093 # of Records: 36,601,939
% of Breaches: 100.0 %of Records: 100.0%

2016 Breaches Identified by the ITRC as of: 1/18/2017

Total Breaches: 1,093
Records Exposed: 36,601,939

The ITRC Breach database is updated on a daily basis, and published to our website on each Tuesday. Unless noted otherwise, each report includes breaches that occurred in the year of the report name (such as "2016 Breach List"), or became public in the report name year, but were not public in the previous year. Each item must be previously published by a credible source, such as Attorney General's website, TV, radio, press, etc. The item will not be included at all if ITRC is not certain that the source is real and credible. We include in each item a link or source of the article, and the information presented by that article. Many times, we have attributions from a multitude of media sources and media outlets. ITRC sticks to the facts as reported, and does not add or subtract from the previously published information. When the number of exposed records is not reported, we note that fact. Note: For data breach incidents involving only emails, user names, and/or passwords, the number of records are not included in the overall total number of records.

What is a breach? A breach is defined as an event in which an individual's name plus Social Security Number (SSN), driver's license number, medical record, or a financial record/credit/debit card is potentially put at risk – either in electronic or paper format.

The ITRC Breach Report presents individual information about data exposure events and running totals for the year. The ITRC Breach Stats Report develops some statistics based upon the type of entity involved in the data exposure.



The ITRC would like to thank CyberScout for its financial support of the ITRC Breach Report, ITRC Breach Stats Report and all supplemental breach reports.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-37	Seirus Innovation	CA	2/5/2016	Electronic	Business	Yes - Unknown #	Unknown

On November 26, 2015, we were notified by the company managing our e-commerce platform that it detected an unauthorized script on the site. The script collected the names, address, email address and credit card information of the customers who made online purchases between November 12 and November 26, 2015. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Seirus Innovation
Article URL: <https://dojmt.gov/wp-content/uploads/Seirus-Innovative-Accessories.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-36	Tetra Technologies	TX	2/16/2016	Electronic	Business	Yes - Unknown #	Unknown

The company believes that on Thursday, February 4, 2016, a list containing some information about you was unintentionally distributed via electronic means outside the company's computer system on which the information was stored. We believe that the information may have included your TETRA employee ID number, first and last name, date of birth, Social Security Number (for U.S. citizens and residents only), and home address. It is also possible that salary information may have been disclosed. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Tetra Technologies
Article URL: <https://dojmt.gov/wp-content/uploads/Tetra-Technologies.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-35	L4 Digital	WA	2/24/2016	Electronic	Business	Yes - Unknown #	Unknown

As you may know, L4 suffered a break-in last September, and several pieces of equipment were stolen. We recently realized that the stolen equipment included a laptop that was no longer in use, but we now believe that it was synchronized with folders in the cloud that contained your personal information. The files that may have been accessible on the laptop include your name, address, social security number, and records documenting the information you supplied to comply with Form I-9 (typically your driver's license number or passport number). (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: L4 Digital
Article URL: <https://dojmt.gov/wp-content/uploads/L4-Digital.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-34	Numerex Corporation	GA	3/4/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to give you notice of a recent incident that may have resulted in the compromise of your personal information - including your social security number, home addresses, and 2015 income. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Numerex Corporation
Article URL: <https://dojmt.gov/wp-content/uploads/Numerix.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-33	Maxim Crane Works	CA	3/11/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 2, 2016, a Maxim employee received a fraudulent email disguised as a legitimate one. The employee responded to the email, believing it to contain a legitimate request, and attached tax forms containing personal information, including name, address, income information, and Social Security numbers. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Maxim Crane Works
Article URL: <https://dojmt.gov/wp-content/uploads/Maxim-Crane-Works.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-32	Engineering Solutions & Products	VA	3/14/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 29, 2016, we became aware of a data breach by which we believe a third party obtained access to copies of your 2015 W-2 income and tax withholding statements. This information was stolen by third parties utilizing criminal phishing techniques. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Engineering Solutions & Products
Article URL: <https://dojmt.gov/wp-content/uploads/Engineering-Solutions-Products.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-31	PayneWest Insurance	MT	3/17/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 15, PayneWest Insurance ("PayneWest") learned that an unidentified attacker had used an email phishing scheme to attempt to obtain access to personal information relating to current and former PayneWest employees. The attacker sent an email message that was carefully designed to appear as though it had been sent by a PayneWest executive, requesting that a PayneWest employee forward 2015 W-2 forms to the executive. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: PayneWest Insurance
Article URL: <https://dojmt.gov/wp-content/uploads/PayneWest.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-30	Northern State Bank	WI	3/17/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On February 8, 2016, Northern State discovered that an unauthorized person stole credentials belonging to a Northern State employee. The credentials were used to log into Northern State's TransUnion account, where the unauthorized person pulled TransUnion credit reports. The unauthorized individual accessed and acquired a copy of your TransUnion credit report. This report included your full name, Social Security number, current and former addresses, date of birth, and credit score. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Northern State Bank
Article URL: <https://dojmt.gov/wp-content/uploads/Northern-State-Bank-supplement.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-29	Road and Highway Builders, LLC	NV	3/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 25, 2016, Road and Highway learned that an email with an attachment containing some personal information of certain Road and Highway employees had been sent to other Road and Highway employees.
What Information Was Involved? The attachment to the email contained personal information relating to certain Road and Highway employees including your name, driver's license number, and date of birth. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Road and Highway Builders, LLC
Article URL: <https://dojmt.gov/wp-content/uploads/Road-and-Highway-Builders-Sterling-Construction.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-28	GlaxoSmithKline	PA	3/25/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 14, 2016, GSK was informed by our third party vendor that personal data of some GSK current and former US employees may have been accessed. GSK was notified as one of several of the vendor's clients who experienced a data breach through a vendor that stores W-2 and historical pay data for us. It appears that W-2 information, including social security number, name, address, and income information was illegally accessed; date of birth also was exposed. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: GlaxoSmithKline
Article URL: <https://dojmt.gov/wp-content/uploads/GlaxoSmithKline-GSK.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 3 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-27	Armstrong, Backus & Co., LLP / myPay Solutions	TX	3/25/2016	Electronic	Business	Yes - Unknown #	Unknown

We have recently learned that the username and password that one of our staff members uses to access myPay Solutions was compromised at some point during January 2016. The unauthorized person(s) then used these credentials to login to myPay Solutions and, we believe, access copies of your employer's W-2 Forms on January 24 and February 7, 2016, including yours. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Armstrong, Backus & Co., LLP / myPay Solutions
Article URL: <https://dojmt.gov/wp-content/uploads/Armstrong-Backus-Co.-myPay-Solutions.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-26	Great Falls Clinic	MT	4/1/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On March 24, 2016, it was discovered that employee W-2 information for the year 2015 was sent in a password protected attachment to an email address outside of this organization. We have learned that your personal information, including name, address, date of birth, and social security may have been compromised. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Great Falls Clinic
Article URL: <https://dojmt.gov/wp-content/uploads/Great-Falls-Clinic.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-25	Next Generation Tax and Accounting	NE	4/6/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 15, 2016, our information technology vendor detected an unauthorized access to the NGTA server, potentially impacting the security of the information contained within it. We can confirm that the compromised server contained your full name, address, and Social Security number and may have included your date of birth and bank account number. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Next Generation Tax and Accounting
Article URL: <https://dojmt.gov/wp-content/uploads/Next-Generation-Tax-and-Accounting.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-24	Midland Paper Packaging & Supplies	IL	4/6/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to make you aware that on Monday April 4, 2016, Midland Paper Packaging & Supplies was the victim of a fraudulent scheme which appears to have resulted in the mistaken release of your W2 form for the year ending December 31, 2015. What Information Was Involved? This incident may impact not only your tax return and refund, but also the personal information contained in your W2 form, including your first and last name, home address, and social security number. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Midland Paper Packaging & Supplies
Article URL: <https://dojmt.gov/wp-content/uploads/Midland-Paper-Packaging-Supplies.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-23	Rule Steel	ID	4/15/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 6, 2016, our company suffered a disclosure of employee information through what is known as a spear-phishing attack. A thief pretending to be me mimicked my company email address and wrote to our Human Resources department requesting a list of Rule Steel's employees for 2014 and 2015 and their dates of birth, salaries, employee identification numbers, Social Security numbers, and addresses. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Rule Steel
Article URL: <https://dojmt.gov/wp-content/uploads/Rule-Steel.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-22	Pioneer News Group	WA	4/12/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 12, 2016 a company-issued laptop was stolen from an employee's car. Unfortunately, the employee's responsibilities required access to personnel information, and the laptop contained personally identifiable information pertaining to employees. It is possible that information such as your name, address, date of birth, and Social Security number was contained on the stolen laptop. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: Pioneer News Group
 Article URL: <https://dojmt.gov/wp-content/uploads/Pioneer-News-Group.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-21	Prime Therapeutics	MN	4/18/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that an unauthorized third party accessed certain information on SeeMyW2.com, a website hosted by Ceridian Corporation a third party vendor. The website allows Prime employees (current and former) to view their W-2 forms online. The personal information that may have been accessed include your name, postal address and Social Security number, and the incident may have resulted in the filing of false tax returns for certain Prime employees. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: Prime Therapeutics
 Article URL: <https://dojmt.gov/wp-content/uploads/Prime-Therapeutics.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-20	Addus HomeCare	IL	4/15/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to make you aware that on March 31, 2016 Addus HomeCare was the victim of a fraudulent scheme which appears to have resulted in the unauthorized acquisition of the personal information contained in your W2 form for the year ending December 31, 2015. This incident may impact not only your tax return and refund, but also the personal information contained in your W2 form, including your first and last name, home address, and social security number. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: Addus HomeCare
 Article URL: <https://dojmt.gov/wp-content/uploads/Addus-HomeCare.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-19	Glu Mobile	CA	6/1/2016	Electronic	Business	Yes - Unknown #	Unknown

On Saturday, May 21, 2016, Glu Mobile learned that the day before, Friday, May 20, 2016, a Glu employee was targeted by an email "spear phishing" scam in which a cyber-criminal impersonated me and requested that 2015 IRS Forms W-2 information be uploaded to a website. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: Glu Mobile
 Article URL: <https://dojmt.gov/wp-content/uploads/Glu-Mobile.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-18	Leavitt Group	UT	4/7/2016	Electronic	Business	Yes - Unknown #	Unknown

Tuesday afternoon, the Leavitt Group's Benefits Department was collecting from some of our staff information on evidence of insurability for term-life coverage. During that process, the Department inadvertently emailed to a very small, isolated group of Leavitt staff an Excel file containing the names and Social Security numbers of a number of current Leavitt employees, including yours. We discovered the error shortly after the email was sent and deleted the information from the recipients' email accounts. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: Leavitt Group
 Article URL: <https://dojmt.gov/wp-content/uploads/Leavitt-Group.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-17	Distinct Software Solutions dba Golf18Network	TX	5/10/2016	Electronic	Business	Yes - Unknown #	Unknown

We are sending this notice to inform you that we recently detected an intrusion into the Golf18 Network payment system (a "Hack"). During the intrusion, an unauthorized third party (a "hacker") temporarily penetrated our checkout system and had access to the following personal information: name, mailing address, email address, phone number, and credit card details. The breach appears to have occurred over a three week period beginning on April 19th. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Distinct Software Solutions dba Golf18Network
Article URL: <https://dojmt.gov/wp-content/uploads/Distinct-Software-Solutions-dba-Golf-18-Network.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-16	MKK Consulting	CO	5/11/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 6, 2016 we discovered that on February 19, 2016, as a result of a phishing email received by one of our employees appearing to come from MKK's President/CEO, an unauthorized third party received an electronic file containing certain information on current and former employees who received employment earnings in 2015 from MKK Consulting Engineers, Inc. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: MKK Consulting
Article URL: <https://dojmt.gov/wp-content/uploads/MKK-Consulting-Engineers.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-15	Curse, Inc.	AL	5/11/2016	Electronic	Business	Yes - Unknown #	Unknown

On or about April 11, 2016, a Curse employee inadvertently sent your 1099-MISC form for the 2015 tax year to an unintended recipient. Curse learned of the incident on the same day. What Information Was Involved? The affected information included on the 1099-MISC tax form includes information such as your name and address, identification number (such as social security number or taxpayer identification number) and financial information such as compensation and federal and state income tax withheld. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Curse, Inc.
Article URL: <https://dojmt.gov/wp-content/uploads/Curse.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-14	Renville County Hospital & Clinics	MN	5/31/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On April 13, 2016 Renville County Hospital & Clinics was notified that an unauthorized user accessed the vendor portal that stores the 2015 W-2, form 1095 and payroll information. At this point in the investigation, it is unclear if your information was accessed. If your information was accessed, it would have contained your personal information, including your direct deposit information, which included your bank account number and routing information, as well as your 2015 W-2 which includes: your full name, address, and Social Security number. In addition, the file would have contained your form 1095, which includes your personal information, as set forth above, and your date of birth, and the personal information of your spouse and any dependents. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Renville County Hospital & Clinics
Article URL: <https://dojmt.gov/wp-content/uploads/Renville-County-Hospital-Clinics.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-13	Southcentral Foundation	AK	6/17/2016	Electronic	Business	Yes - Unknown #	Unknown

SCF used an outside vendor, Greenshades, to provide services including preparation and online distribution of our employee IRS Form W-2. After receiving reports from some employees of fraudulent tax filings in their names, we shut down user access to the information on Greenshades' systems. If you are a current, former or retired employee who received a 2015 IRS Form W-2 from SCF, this incident may affect the security of information contained on your IRS Form W-2, which includes employee name, Social Security number, wage information and withholding information. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: Southcentral Foundation
 Article URL: <https://dojmt.gov/wp-content/uploads/Southcentral-Foundation-SCF.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-12	Medtronic	MN	7/8/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A Medtronic website contained a file with personal information associated with the MiniMed Ambassador program that was inadvertently accessible on the internet. As soon as we became aware of this issue, we worked to correct it. What Information Was Involved: The file contained your name, address, demographic information and healthcare providers' names. It also contained answers on the MiniMed Ambassador volunteer program application. The file did not contain your social security number or payment card information. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: Medtronic
 Article URL: <https://dojmt.gov/wp-content/uploads/Medtronic.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-11	Career Education Corporation	IL	7/11/2016	Electronic	Educational	Yes - Unknown #	Unknown

On June 16, 2016 we believe a contractor for the company may have copied a file from the company's secure network. The copied file contained names, addresses and Social Security numbers. (End of year entry – MT AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: Career Education Corporation
 Article URL: <https://dojmt.gov/wp-content/uploads/Career-Education-Corporation.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-10	Teikyo Loretto Heights University dba Colorado	CO	12/28/2016	Electronic	Educational	Yes - Unknown #	Unknown

On November 23, 2016, CHU learned from our third-party vendor that hosts our college management system that an unauthorized person or persons may have created and accessed a backup of CHU's college management system.

Attribution 1 Publication: NH AG's office Author:
 Article Title: Teikyo Loretto Heights University dba Colorado Heights University
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/teikyo-loretto-heights-20162323.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-09	Gustafson & Wargo, CPAs, LLP	NY	12/2/2016	Electronic	Business	Yes - Unknown #	Unknown

On or around October 15, 2016, we discovered activity on our network that occurred on October 13, 2016 that did not appear to be legitimate, including the unauthorized use of employee credentials into our network. Through this activity, files containing personal information for our clients were accessible. The information the unidentified individual may have accessed included your name, address, tax information, Social Security number, date of birth, and/or banking information.

Attribution 1 Publication: NH AG's office Author:
 Article Title: Gustafson & Wargo, CPAs, LLP
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/gustafson-wargo-20161202.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-08	American Pharmacists Association / Comnet	DC	12/29/2016	Electronic	Business	Yes - Unknown #	Unknown

Our law firm represents the American Pharmacists Association ("APhA"), a tax exempt entity under Section 501(c)(6) of the Internal Revenue Code, which is a national professional society of pharmacists, scientists, students, technicians, and others interested in advancing the profession. Pursuant to N.H. Rev. Stat. § 359-C:20, APhA hereby notifies you that Comnet Marketing Group, Inc. ("Comnet"), an APhA vendor, experienced a data security breach involving ransomware malware and unauthorized access on or about April 23-24, 2016 that may have involved the personal information of two New Hampshire residents.

Attribution 1 Publication: NH AG's office Author:
Article Title: American Pharmacists Association / Comnet
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/comnet-marketing-20161229.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-07	Hash, O'Brien, Biby & Murray PLLP	MT	12/19/2016	Electronic	Business	Yes - Unknown #	Unknown

We are contacting you to notify you that during the morning hours of December 13, 2016, our office was burglarized. Personal items were stolen, as well as computers. Your personal information may have been stored on the stolen computers. This theft has caused us to be concerned for the security of our electronically stored information.

Attribution 1 Publication: MT AG's office Author:
Article Title: Hash, O'Brien, Biby & Murray PLLP
Article URL: <https://dojmt.gov/wp-content/uploads/Hash-O'Brien-Biby-Murray-PLLP.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-06	Cascade Management, Inc.	OR	12/29/2016	Electronic	Business	Yes - Published #	3,465

Our client, Cascade Management., Inc. ("Cascade"), submits this notice after learning of a security incident that may have involved personal information for Oregon residents.

Attribution 1 Publication: OR AG's office / MT AG's office Author:
Article Title: Cascade Management, Inc.
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1750869862>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-05	Washington National Insurance Company	IN	11/18/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,458

Washington National Insurance Company IN Health Plan 1458 11/18/2016 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Washington National Insurance Company
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-04	Washington Health System	PA	12/2/2016	Electronic	Medical/Healthcare	Yes - Published #	544

Washington Health System PA Healthcare Provider 544 12/02/2016 Theft Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: Washington Health System
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-03	ADVANTAGE Health Solutions	IN	12/22/2016	Electronic	Medical/Healthcare	Yes - Published #	2,387

ADVANTAGE Health Solutions IN Health Plan 2387 12/22/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: ADVANTAGE Health Solutions
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 8 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-02	Sheet Metal Workers' Local Union No. 104	CA	12/30/2016	Electronic	Business	Yes - Unknown #	Unknown

Attribution 1 Publication: CA AG's office Author:
Article Title: Sheet Metal Workers' Local Union No. 104
Article URL: https://oag.ca.gov/system/files/Sheetworkers%20Local%20104%20Notice%20ONLY-%20CA%20original%20_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161231-01	Pentagon / Potomac Healthcare Solutions	VA	12/31/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

A Pentagon subcontractor has exposed reams of highly sensitive details belonging to active military healthcare professionals online, some of which hold top-secret security clearances. The bulk of the data is made up of military personnel files and lists of physical and mental health support staff, including nurses, doctors, and mental health professionals. Names, contract types, Social Security numbers, and duty start dates -- dating back to 1998 -- as well as billet numbers that detail the living quarters for when staff are not on active duty, are all included in the information leak.

Attribution 1 Publication: zdnet.com Author:
Article Title: US government subcontractor leaks confidential military personnel data
Article URL: <http://www.zdnet.com/article/us-government-subcontractor-leaks-confidential-military-personnel-data/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161230-01	Columbia County School District	GA	12/25/2016	Electronic	Educational	Yes - Unknown #	Unknown

Some Columbia County Schools employees were encouraged to increase security on personal information accounts after being notified by district officials of a possible data breach in late November, in which a third party might have had access to personal information, including Social Security numbers.

Attribution 1 Publication: newstimes.augusta.com Author:
Article Title: Schools report server hack jeopardizes private employee information
Article URL: <http://newstimes.augusta.com/news/2016-12-25/schools-report-server-hack-jeopardizes-private-employee-information>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-23	Venture Logistics	IN	11/23/2016	Electronic	Business	Yes - Unknown #	Unknown

On November 14, 2016 an e-mail with an unencrypted attachment containing your name, social security number, personal e-mail address, date of hire and your benefit elections for 2016 was sent to 360 Company employees.

Attribution 1 Publication: NH AG's office Author:
Article Title: Venture Logistics
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/venture-logistics-20161206.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-22	Upper Connecticut Valley Hospital	NH	12/23/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On October 7, 2016, UCVH learned of an incident that occurred on September 23, 2016 in which a third party may have gained access to personal information contained on a vendor's computer and local network when the computer was infected with malicious software. CVH's investigation determined that the personal information that may have been accessed included the names, addresses, telephone numbers, dates of birth, and social security numbers of two New Hampshire residents.

Attribution 1 Publication: NH AG's office Author:
Article Title: Upper Connecticut Valley Hospital
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/upper-connecticut-valley-hospital-20161223.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 9 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-21	Julep Beauty, Inc.	WA	12/9/2016	Electronic	Business	Yes - Unknown #	Unknown

Late on November 8, 2016, we discovered an unauthorized third party hacker gained access to a portion of our website. The hacker was able to divert certain data entered on our website between, approximately, November 6-8, 2016 from our normal tokenized payment data pathway into a pathway created by the hacker.

What Information Was Involved? The hacker was able to divert payment card information such as your card number and other information typically necessary to making a purchase. This appears to have been limited to new customers or existing customers who updated their information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Julep Beauty, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/julep-beauty-20161209.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-20	Indique	MA	12/5/2016	Electronic	Business	Yes - Published #	1,500

We are writing to notify you that a breach of security/unauthorized acquisition of your personal information may have occurred between September 1st, 2016 and November 28th, 2016. The breach was caused by third party actors re-writing sections of our website code sometime after September 1st but before November 1st 2016. The hack allowed consumer credit card information to be captured simultaneously as it was entered on the site.

Attribution 1 Publication: NH AG's office Author:
Article Title: Indique
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/indique-hair-20161205.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-19	Gorilla Glue Company	OH	12/14/2016	Electronic	Business	Yes - Unknown #	Unknown

On November 14, 2016, we discovered an unauthorized intrusion into our computer systems which allowed access to our email and network drives. WHAT INFORMATION WAS INVOLVED: While our investigation is ongoing, we have evidence to indicate that certain personal information such as names, social security numbers, and addresses of current and former employees in emails and other documents stored on the network drives may have been exposed and accessed.

Attribution 1 Publication: NH AG's office Author:
Article Title: Gorilla Glue Company
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/gorilla-glue-20161214.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-18	Fujitsu Computer Products of America, Inc.	CA	12/14/2016	Electronic	Business	Yes - Unknown #	Unknown

Specifically, we recently discovered that personal data collected through our website, store.fcmafujitsu.com (the "Webstore"), may have been compromised. Through our investigation, we have determined that the unauthorized third party accessed names and payment card information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Fujitsu Computer Products of America, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/fujitsu-computer-20161214.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-17	Breville USA	CA	12/9/2016	Electronic	Business	Yes - Unknown #	Unknown

On December 5, 2016, we discovered and removed malware on our e-commerce website that was placed there on December 1, 2016. The malware could have obtained access to information you submitted to the website between those dates, such as billing and shipping names, email addresses, telephone numbers, and addresses, and payment card number, CVV, and expiration date.

Attribution 1 Publication: NH AG's office Author:
Article Title: Breville USA
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/breville-usa-20161213.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-16	Providence Health & Services	WA	12/29/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Between Oct. 25, 2016 and Oct. 28, 2016, an unauthorized individual accessed the paging system used by Providence and several other health care organizations, public safety departments and businesses. Information related to you was intercepted and displayed on [Insert Disclosure Date]. The information displayed about you included your demographic information (which could include your name, date of birth, and room number), and may have limited clinical information (which could include medication, symptoms, medical record numbers, procedures, or diagnosis.)

Attribution 1 Publication: OR AG's office / databreaches.net Author:
Article Title: Providence Health & Services
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/170839689>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-15	Safe for Home Products LLC dba Naturepedic	OH	12/28/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 28, 2016, during an extensive scan, we learned that encrypted malware had been placed on our www.naturepedic.com website. What information was involved? The malware copied the information entered on our website to create online accounts and to place orders between June 6 and October 28, 2016, including a customer's name, address, telephone number, and credit card information.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Naturepedic
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Naturepedic%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-14	Georgia Tech	GA	12/22/2016	Electronic	Educational	Yes - Unknown #	Unknown

On Dec. 12, a Georgia Tech employee conducted research on a trusted website that had been compromised by a malicious software known as ransomware. The ransomware infiltrated the employee's computer, which was connected to Georgia Tech's network, allowing access to a variety of files — some of which included sensitive, personal information of current and past Georgia Tech employees

Attribution 1 Publication: news.gatech.edu Author:
Article Title: Human Resources Notifies Employees of Data Breach
Article URL: <http://www.news.gatech.edu/2016/12/22/human-resources-notifies-employees-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-13	Forsyth County Tax Commission	GA	12/22/2016	Electronic	Government/Military	Yes - Published #	19,793

A security breach at the Forsyth County Tax Commissioners office led to the inadvertent release Social Security numbers of nearly 20,000 residents.

Attribution 1 Publication: databreaches.net / myajc.com Author:
Article Title: Forsyth County investigates information breach
Article URL: <http://www.myajc.com/news/local/forsyth-county-investigates-information-breach/cv8De4twCRcGcmGmw4QSOI/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-12	University of Maine	ME	12/23/2016	Electronic	Educational	Yes - Published #	86

The University of Maine reports some of their staff and students have been victims of cyber criminals. According to the school, 86 individuals were tricked into providing their login credentials in an online phishing attack. Personal passwords were given out to access an online document that was actually fake. We're told the cyber criminals then used that information to access university accounts, hoping to find bank account and social security numbers.

Attribution 1 Publication: wabi.tv Author:
Article Title: UMaine Systems Reports Phishing Attack
Article URL: <https://wabi.tv/2016/12/23/umaine-systems-reports-phishing-attack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-11	WestPark Capital	CA	9/27/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

So now to the hack they revealed: WestPark Capital in California, an international investment banking and securities brokerage firm that was founded in 1995. TDO provided a sample of documents as proof of claim, including an image of a retainer check and a number of confidential files, including several background checks on individuals by BackTrack, non-disclosure agreements, and other internal documents.

Attribution 1 Publication: databreaches.net Author:
Article Title: WestPark Capital (TDO)
Article URL: <https://www.databreaches.net/two-more-hacks-with-ransom-demands-but-is-anyone-paying-part-2/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-10	V.I. Pay, Inc.	MI	9/27/2016	Electronic	Business	Yes - Unknown #	Unknown

In an encrypted chat on September 20, "Return" claimed that he had hacked a payroll processing firm in Grandville, Michigan, V.I. Pay, Inc. As he has done in other cases, "Return" provided a large (147 mb) sample of the data he claims to have acquired. The sample includes numerous spread sheets from named clients, files with personal and financial information, login credentials, and more. The files in the sample contain a slew of personal data, such as a spreadsheet with commissions paid to a realty firm's employees, and another spreadsheet purportedly from another firm's 401K plan that includes 111 rows with the participants' name, postal and email addresses, Social Security number, date of birth, amount of employee and employer contributions to the plan, and telephone number.

Attribution 1 Publication: databreaches.net Author:
Article Title: V.I. Pay, Inc. (TDO)
Article URL: <https://www.databreaches.net/two-more-hacks-with-ransom-demands-but-is-anyone-paying-part-1/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-09	Brandywine Pediatrics. P.A.	DE	12/29/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

The practice notified patients on December 23 that on October 25, they had discovered that their file server was inaccessible due to a computer virus. They did not indicate what type of ransomware was involved. Brandywine reports that were able to immediately restore their files from backup tapes, but a forensic computer expert hired to assist with their investigation subsequently determined that patient files containing name, address, and medical information, may have been accessed by an unauthorized person. The files did not include any Social Security numbers or payment card information.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: Hit by ransomware, Brandywine Pediatrics recovers quickly and notifies patients
Article URL: <https://www.databreaches.net/hit-by-ransomware-brandywine-pediatrics-recovers-quickly-and-notifies-patients/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-08	Atmore Community Hospital / Infirmary Health	AL	12/29/2016	Electronic	Medical/Healthcare	Yes - Published #	1,000

An Atmore Community Hospital employee was terminated for accessing the electronic record of approximately 1,000 patients without an appropriate work-related reason, according to a press release from Infirmary Health.

Attribution 1 Publication: databreaches.net / atmoreadvance.com Author:
Article Title: ACH fires employee
Article URL: <http://www.atmoreadvance.com/2016/12/28/ach-fires-employee/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 12 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-07	Graphik Dimensions, Ltd.	NC	11/30/2016	Electronic	Business	Yes - Unknown #	Unknown

On or around November 9, 2016, Graphik Dimensions was advised that it had been identified as a common point of purchase for credit card fraud. On or around November 29, 2016, Graphik Dimensions' investigation confirmed that an unidentified third party had injected malicious code into the pictureframes.com e-commerce site. The malicious code enabled the unidentified third party to acquire credit card information while the purchase took place.

Attribution 1 Publication: CA AG's office / VT AG's office / NH AG' Author:
Article Title: Graphik Dimensions, Ltd.
Article URL: https://oag.ca.gov/system/files/Graphik%20-%20CA%20Exhibit%201%20for%20Online%20Forms_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-06	Topps Company, Inc.	NY	7/30/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 12, 2016, Topps became aware that one or more intruders gained unauthorized access to its website. WHAT INFORMATION WAS INVOLVED?

This incident may have compromised names, addresses, e-mail addresses, phone numbers, credit or debit card numbers, card expiration dates, and card verification numbers for customers as they placed orders through the Topps website between approximately July 30, 2016 and October 12, 2016.

Attribution 1 Publication: CA AG's office / VT AG's office / MT AG' Author:
Article Title: Topps Company, Inc.
Article URL: https://oag.ca.gov/system/files/Breach%28CAFormNotice%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-05	Claremont University Consortium	CA	12/22/2016	Electronic	Educational	Yes - Unknown #	Unknown

On November 15, 2016, several items, including a password-protected laptop, were stolen from a Claremont University Consortium employee's locked vehicle. The theft was discovered the same day and the employee promptly notified the College and the Berkeley Police Department. We have been working with law enforcement but, to date, they have been unable to locate the suspects or the stolen items. What information was involved? Our investigation has confirmed that the stolen laptop may have contained information regarding your 1099 tax form, including your name, address, date of birth, and Social Security number.

Attribution 1 Publication: CA AG's office / MT AG's office Author:
Article Title: Claremont University Consortium
Article URL: https://oag.ca.gov/system/files/Claremont%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-04	Department of Health and Human Services / New	NH	12/27/2016	Electronic	Government/Military	Yes - Published #	15,000

A former patient at New Hampshire's state psychiatric hospital posted confidential information about thousands of people on a social media website, health officials said Tuesday. Department of Health and Human Services Commissioner Jeffrey Meyers said a patient using a computer in the New Hampshire Hospital library in October 2015 accessed information on as many as 15,000 people who had received department services

Attribution 1 Publication: sacbee.com / NH AG's office Author:
Article Title: New Hampshire psychiatric patient accused of data breach
Article URL: <http://www.sacbee.com/news/business/technology/article123150334.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-03	InterContinental Hotels Group	GA	12/28/2016	Electronic	Business	Yes - Unknown #	Unknown

InterContinental Hotels Group (IHG), the parent company for more than 5,000 hotels worldwide including Holiday Inn, says it is investigating claims of a possible credit card breach at some U.S. locations.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Holiday Inn Parent IHG Probes Breach Claims
Article URL: <https://krebsonsecurity.com/2016/12/holiday-inn-parent-ihg-probes-breach-claims/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-02	Nevada Division of Public and Behavioral Health	NV	12/29/2016	Electronic	Government/Military	Yes - Published #	11,700

Nevada took its medical marijuana program database off the internet this week after the Social Security numbers and other sensitive information involving thousands of dispensary applicants were inadvertently leaked online. A vulnerability affecting a web portal used by the state's medical weed program resulted in more than 11,700 dispensary applications being publicly accessible prior to the database being disabled this week, security researcher Justin Schafer said Wednesday.

Attribution 1 Publication: nakedsecurity.sophos.com / Washington Author:
Article Title: Nevada takes medical marijuana database offline after data breach affects dispensary applicants
Article URL: <http://www.washingtontimes.com/news/2016/dec/29/nevada-takes-medical-marijuana-database-offline-af/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161229-01	Desert Care Family and Sports Medicine	AZ	12/20/2016	Electronic	Medical/Healthcare	Yes - Published #	500

On December 20, the center notified HHS that 500 patients were being notified that their server had been infected in August 2016. Of note, not only were the data on the server encrypted – including patient records – but Desert Care took the server to several IT specialists who were all reportedly unable to break the encryption.

Attribution 1 Publication: hhs.gov / databreaches.net Author:
Article Title: Desert Care Family and Sports Medicine
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161222-07	Southcentral Foundation	AK	12/16/2016	Electronic	Medical/Healthcare	Yes - Published #	14,719

On October 18, 2016, SCF became aware that some employee email accounts might be accessible to persons outside the organization as a result of a cyber security attack.

Attribution 1 Publication: MT AG's office / databreaches.net / hhs.gov Author:
Article Title: Southcentral Foundation
Article URL: <https://dojmt.gov/wp-content/uploads/Southcentral-Foundation-SCF-2.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161222-06	Federal Savings Bank	IL	12/20/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

TFSB recently discovered that an employee's e-mail account was criminally hacked and then used to send phishing e-mails. That personal information may include your name, mailing address, Social Security number, date of birth, driver's license number, bank account or other financial account number without any passcode or security code, and credit or debit card number.

Attribution 1 Publication: MT AG's office Author:
Article Title: Federal Savings Bank
Article URL: <https://dojmt.gov/wp-content/uploads/The-Federal-Savings-Bank.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161222-05	Bomberg, Roach & Hanson, PLLC	MN	12/16/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 13, 2016, we discovered that an unauthorized individual had gained access to our electronic file storage system. We also conducted an investigation and determined that files that the individual may have accessed could have contained your name, address, date of birth, Social Security number, and financial account information. We immediately contacted the IRS, who has flagged any potentially affected taxpayer accounts to protect against unauthorized activity on those accounts.

Attribution 1 Publication: MT AG's office / NH AG's office Author:
 Article Title: Bomberg, Roach & Hanson, PLLC
 Article URL: <https://dojmt.gov/wp-content/uploads/Bomberg-Roach-Hanson-PLLC.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161222-04	Luther College	IA	12/20/2016	Electronic	Educational	Yes - Unknown #	Unknown

On October 12, 2016, we discovered that Luther College had become the target of a phishing email campaign and that a few Luther College employees had clicked on the phishing emails and entered their credentials. These workstation computer files and email accounts contained, among other things, personally identifiable information of certain individuals related to Luther College. While we have no evidence that the unauthorized individual or individuals actually accessed or acquired your information, we have confirmed that your name and Bank Account Number, Bank Name were accessible to the intruder.

Attribution 1 Publication: MT AG's office / NH AG's office Author:
 Article Title: Luther College
 Article URL: <https://dojmt.gov/wp-content/uploads/Luther-College.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161222-03	Henry County Health Department Home Health and	OH	12/22/2016	Electronic	Medical/Healthcare	Yes - Published #	500

More than 500 patients served by Henry County Health Department Home Health and Hospice are being notified after a nurse's laptop and paperwork was stolen from her garaged car on October 22.

Attribution 1 Publication: databreaches.net Author:
 Article Title: Henry County home health and hospice patients' records stolen
 Article URL: <https://www.databreaches.net/oh-henry-county-home-health-and-hospice-patients-records-stolen/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161222-02	Fairbanks Hospital	IN	12/22/2016	Electronic	Medical/Healthcare	Yes - Published #	12,994

On October 18, 2016, Fairbanks became aware that some files on our internal network that contained patient information were electronically accessible to Fairbanks employees, including employees who were not intended to have access to patient information. Based upon our investigation, it was determined that the following types of patient information were contained on one or more files on our network that were impacted by this issue: name, Social Security number, date of birth, contact information, patient identification number, diagnosis, treatment information, health insurance information, and information relating to initial admission and scheduling of appointments.

Attribution 1 Publication: databreaches.net / hospital website / hh Author:
 Article Title: STATEMENT REGARDING FAIRBANKS HOSPITAL'S
 Article URL: <http://www.fairbanksd.org/statement-regarding-fairbanks-hospitals-recent-data-privacy-event/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161222-01	Dover Federal Credit Union	DE	12/22/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On September 20, 2016, DFCU learned that an employee had transferred DFCU files to the employee's personal Dropbox account to access the information from the employee's home computer for business purposes. The information included your name, address, DFCU account number, and your Social Security number.

Attribution 1 Publication: CA AG's office / MT AG's office Author:
 Article Title: Dover Federal Credit Union
 Article URL: https://oag.ca.gov/system/files/DFCU%20CA%20Adult%20Letter%20Sample_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161221-05	Western Union Financial Services, Inc.	CO	12/20/2016	Electronic	Business	Yes - Published #	15,700

Hackers stole credit and debit card information from 15,700 online customers of Western Union, whose Web site was unprotected while undergoing maintenance. Western Union said the problem was caused by human error and not an inherent technical flaw.

Attribution 1 Publication: CA AG's office / ABCnews.go.com Author:
Article Title: Western Union Financial Services, Inc.
Article URL: <http://abcnews.go.com/US/story?id=95806&page=1>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161221-04	Kaiser Permanente	CA	11/28/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

You visited kp.org between November 16 and 28, 2016, and used our online Estimates tool. Due to a system error, there is a small chance that your name, age, address, and some information on how much you've spent on health care this year may have been seen by another kp.org user.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Kaiser Permanente
Article URL: https://oag.ca.gov/system/files/Patient%20Notification%20Letter%20-%20DRAFT%2012-20-16_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161221-03	Columbia County School District	GA	12/21/2016	Electronic	Educational	Yes - Unknown #	Unknown

A message was sent out to Columbia County School District employees and students about a possible data breach. According to a release, on Nov. 28, the district confirmed one of their servers was compromised by an outside entity. The school district said Wednesday that no student data was on the server but it did contain some confidential employee information, including personal information such as names, Social Security numbers, and birth dates of their employees, their dependents, spouses, and any other life, dental, or vision insurances beneficiaries.

Attribution 1 Publication: wrdw.com / databreaches.net Author:
Article Title: Possible data breach affects Columbia County School district employees
Article URL: <http://www.wrdw.com/content/news/Possible-data-breach-affects-Columbia-County-School-district-employees-407785>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161221-02	Community Health Plan of Washington	WA	12/21/2016	Electronic	Medical/Healthcare	Yes - Published #	381,534

More than 380,000 current and former members of the Community Health Plan of Washington may have had personal information stolen in a data breach, officials confirmed. A statement released Wednesday by Community Health Plan says, "It appears that names, addresses, dates of birth, Social Security numbers and certain coding information related to health care claims may have been accessed. Banking and credit information was not contained in the data."

Attribution 1 Publication: komonews.com / WA AG's office Author:
Article Title: Data breach at Community Health Plan of Wash. exposes 380,000 members
Article URL: <http://komonews.com/news/local/data-breach-at-community-health-plan-of-wash-exposes-380000-members>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161221-01	University of Nebraska - Lincoln	NE	12/20/2016	Electronic	Educational	Yes - Published #	30,000

University of Nebraska-Lincoln officials emailed students Tuesday to warn them of a security breach. The names, ID numbers and grades of 30,000 current and former students may have been comprised over the last two years, the email read.

Attribution 1 Publication: ketv.com Author:
Article Title: UNL security breach puts thousands of current, former students' information at risk
Article URL: <http://www.ketv.com/article/unl-security-breach-puts-thousands-of-current-former-students-information-at-risk/852243>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-10	United States Fire Insurance Company	NJ	7/21/2016	Electronic	Business	Yes - Unknown #	Unknown

A U.S. Fire employee within the CoverX division had a company cell phone stolen on May 16, 2016. While U.S. Fire's investigation has been unable to determine whether any of the personal information contained in email was viewed or accessed, it does know that the cell phone contained certain personal information in email and/or attachment(s) that included your name, driver's license number and date of birth.

Attribution 1 Publication: MT AG's office Author:
Article Title: United States Fire Insurance Company
Article URL: <https://dojmt.gov/wp-content/uploads/US-Fire-CoverX-Corporation.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-09	American College of Emergency Physicians /	TX	7/22/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to provide you with important information about a recent incident with a third party vendor involving some of your personal information. Based on what ComNet has reported to ACEP, it appears that your personal information, including, your full name, address, and credit card or debit card, or other payment information you used to renew your membership, may have been accessed by an unauthorized third party as a result of the intrusion.

Attribution 1 Publication: MT AG's office Author:
Article Title: American College of Emergency Physicians / ComNet Marketing Group
Article URL: <https://dojmt.gov/wp-content/uploads/American-College-of-Emergency-Physicians-ACEP.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-08	Taleff & Murphy, P.C.	MT	8/10/2016	Electronic	Business	Yes - Unknown #	Unknown

On Wednesday, June 15, 2016, our law office was the subject of a computer "hack" in which access was gained to our data system. We understand the access was made through an attachment to an email, but at this time we do not have any definitive information as to how the access was accomplished.

Attribution 1 Publication: MT AG's office Author:
Article Title: Taleff & Murphy, P.C.
Article URL: <https://dojmt.gov/wp-content/uploads/Taleff-Murphy.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-07	USAA Federal Savings Bank	TX	8/11/2016	Electronic	Business	Yes - Unknown #	Unknown

Between July 23 – 25, 2016, a technical error occurred that may have caused your W-9 form to be displayed to another member for a brief moment. The technical error was corrected and we are taking steps to prevent similar incidents in the future. The personal information involved in this incident may have included your first and last name, address, and social security number.

Attribution 1 Publication: MT AG's office Author:
Article Title: USAA Federal Savings Bank
Article URL: <https://dojmt.gov/wp-content/uploads/USAA-Federal-Savings-Bank.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-06	Green Plains, Inc.	NE	8/1/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 27, 2016, we learned that a password-protected laptop computer issued to one of our employees had been stolen from the employee's vehicle the night before. After conducting a thorough review, we determined that the laptop may have contained vendor forms. To the extent the vendor forms were on this laptop, one of them would have contained your name, address, and banking information.

Attribution 1 Publication: MT AG's office Author:
Article Title: Green Plains, Inc.
Article URL: <https://dojmt.gov/wp-content/uploads/Green-Plains-Inc.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-05	Anderson, Tackman & Company PLC	WI	8/15/2016	Electronic	Business	Yes - Unknown #	Unknown

We are writing to provide you with important information about a recent incident which involves the security of some of your personal information that was supplied to us. Based on our forensic investigation, we can confirm that certain tax returns were accessed, including your tax return that contained your full name, address and Social Security number, and possibly your bank account and routing number.

Attribution 1 Publication: MT AG's office Author:
 Article Title: Anderson, Tackman & Company PLC
 Article URL: <https://dojmt.gov/wp-content/uploads/Anderson-Tackman-Co..pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-04	Matouk Factory Store	MA	8/8/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 22 we detected suspicious activity that occurred on our website between 6/19/2016 and 7/22/2016. Upon learning this, we immediately worked to strengthen security measures throughout the Matouk system. The data accessed during this period may have included personal information such as Name, Billing Address, Phone Number, Email Address and Credit Card information for card number ending in XXX.

Attribution 1 Publication: MT AG's office Author:
 Article Title: Matouk Factory Store
 Article URL: <https://dojmt.gov/wp-content/uploads/Matouk.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-03	Bank of America	NC	3/21/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

An incident occurred on January 19, 2016 that resulted in the disclosure of your information by a former employee who retained your information for business solicitation purposes at their current place of employment. The former employee has confirmed destruction of your information. WHAT INFORMATION WAS INVOLVED: According to our records, the information involved in this incident was related to your mortgage loan application and may have included your first and last name, address, phone number, date of birth, Social Security number, account numbers and account balances.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Bank of America
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266930.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-02	Contact Solutions	VA	3/4/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On February 17, 2016, Contact Solutions, LLC management was notified that Contact Solutions, LLC was the victim of a successful phishing incident that resulting in the unauthorized disclosure of employee information. We believe that your personal information, including name, social security number, wage information may have been among the information that was compromised.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Contact Solutions
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266933.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161220-01	4D Sound Diagnostics	TX	12/20/2016	Electronic	Medical/Healthcare	Yes - Published #	1,000

Unfortunately, and as we're seeing all too often, a cloned server using the Rsync protocol was indexed by Shodan and was available to anyone and everyone because port 873 was open. So what was in the exposed data? For those seeking elective ultrasounds, the files contained client/patient forms with name, date of birth, address, email address, telephone numbers, due date, how many weeks pregnant, physician's name, method of payment, and a permission/consent form asking whether the firm could use the woman's name and the ultrasound image on its web site or for advertising.

Attribution 1 Publication: databreaches.net Author:
 Article Title: Texas firm exposed fetal and patient ultrasounds
 Article URL: <https://www.databreaches.net/texas-firm-exposed-fetal-and-patient-ultrasounds/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 18 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161219-08	Pentagon	DC	12/15/2016	Electronic	Government/Military	Yes - Published #	3,500

Russian hackers struck at the heart of the U.S. military in August 2015 by seizing the e-mail system used by the Joint Chiefs of Staff, CBS News has learned. Within an hour, hackers had seized control of the unclassified e-mail system used by the Pentagon's Joint Staff, the organization of some 3,500 military officers and civilians who work for the Chairman. In that time, the hackers seized the computer credentials of Dempsey and hundreds of other senior officers -- the passwords and electronic signatures they used to sign on to the network.

Attribution 1 Publication: cbsnews.com Author:
Article Title: Russian hack almost brought the U.S. military to its knees
Article URL: <http://www.cbsnews.com/news/russian-hack-almost-brought-the-u-s-military-to-its-knees/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161219-07	Lumiere Place Casino & Hotels / Tropicana St. Louis,	MO	12/15/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that on October 27, 2016, an unauthorized party obtained certain individuals' information from a security report management system at Lumiere Place Casino & Hotels. The information may have included personal information such as names, addresses and Social Security numbers.

Attribution 1 Publication: MT AG's office Author:
Article Title: Lumiere Place Casino & Hotels / Tropicana St. Louis, LLC
Article URL: <https://dojmt.gov/wp-content/uploads/Tropicana-St.-Louis-LLC.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161219-06	UnitedStatesGoldBureau.com	AL	12/15/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 28, 2016, we discovered that unauthorized emails were sent from our marketing email account. We immediately launched an internal investigation and retained third-party forensic experts to assist in the investigation of the incident. The forensic investigators later determined that a server used to store customer contact information was subject to unauthorized access.

Attribution 1 Publication: MT AG's office Author:
Article Title: UnitedStatesGoldBureau.com
Article URL: <https://dojmt.gov/wp-content/uploads/USGB-LLC.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161219-05	Corpus Christi Independent School District	TX	12/17/2016	Electronic	Educational	Yes - Published #	443

The Corpus Christi Independent School District is offering 443 of their former students and one current student free credit monitoring service, after their Social Security numbers were published to the internet.

Attribution 1 Publication: databreaches.net Author:
Article Title: CCISD notifies students of breach of personal info
Article URL: <https://www.databreaches.net/tx-ccisd-notifies-students-of-breach-of-personal-info/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161219-04	Ameriprise	MN	12/16/2016	Electronic	Banking/Credit/Financial	Yes - Published #	350

An advisor working for financial planning giant Ameriprise has inadvertently exposed hundreds of investment portfolios, worth tens of millions of dollars. The data was found on an internet-connected backup drive at the advisor's home, which was set to synchronize over the internet with his primary backup drive at his office. But neither drive had a password, allowing anyone to view sensitive client data.

Attribution 1 Publication: zdnet.com / NH AG's office Author:
Article Title: Ameriprise leak exposes millions of dollars worth of accounts
Article URL: <http://www.zdnet.com/article/ameriprise-leak-exposes-millions-of-dollars-worth-of-accounts/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161219-03	Lynda.com	CA	12/18/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently became aware that an unauthorized third party breached a database that included some of your Lynda.com learning data, such as contact information and courses viewed. We are informing you of this issue out of an abundance of caution. Please know that we have no evidence that this data included your password. And while we have no evidence that your specific account was accessed or that any data has been made publicly available, we wanted to notify you as a precautionary measure.

Attribution 1 Publication: [mspouser.com / databreaches.net](http://mspouser.com/databreaches.net) Author:
Article Title: LinkedIn's Lynda.com starts notifying users about a data breach affecting more than 50 thousand users
Article URL: <https://mspouser.com/linkedin-lynda-com-starts-notifying-users-data-breach-affecting-50-thousand-users/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161219-02	Modern Business Solutions	TX	10/13/2016	Electronic	Business	Yes - Unknown #	Unknown

MBS is a company specializing in providing in-house data management and monetization services to other companies. If you're an MBS customer, then you probably don't even know it, and the 58 million stolen database records could belong to just about anyone. The data was quickly removed each time, but it included complete names, IP addresses, dates of birth, email addresses, vehicle data, and occupations. In other words, the data would be incredibly helpful for conducting further, highly individualized attacks such as identity theft.

Attribution 1 Publication: digitaltrends.com Author:
Article Title: Hacker steals at least 58 million personal records from data management firm
Article URL: <http://www.digitaltrends.com/computing/modern-business-solutions-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161219-01	County of Los Angeles	CA	5/13/2016	Electronic	Government/Military	Yes - Published #	749,017

The County of Los Angeles is notifying 756,000 individuals of a breach that occurred five months ago stemming from a phishing scheme that tricked more than 100 county employees. Bank account and payment card information, Social Security numbers and health-related information was potentially exposed.

Attribution 1 Publication: healthcareinfosecurity.com Author: Marianne Kolbasuk M
Article Title: L.A. County: Major Breach Stemmed from Phishing Attack
Article URL: <http://www.healthcareinfosecurity.com/la-county-major-breach-stemmed-from-phishing-attack-a-9595?rf=2016-12-20-e>

Attribution 2 Publication: CA AG's office / hhs.gov Author:
Article Title: County of Los Angeles
Article URL: https://oag.ca.gov/system/files/LA%20County%20Ad%20CEO%20r16prf_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-17	Coronado Stone Products	CA	2/29/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 2, 2016, an unusual activity was detected on the Company's information system. The Company immediately launched an investigation to determine what information had potentially been affected. A server containing payroll records and information for direct deposit purposes appeared to have been compromise. The affected server contains the employee's name, address, social security number and financial account number (without password, security code, or access code), of two (2) employee's in Maryland.

Attribution 1 Publication: MD AG's office Author:
Article Title: Coronado Stone Products
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266935.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-16	SkyOne Federal Credit Union	CA	3/15/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 4, 2016, we learned that a device containing member information was lost while in transit to our branch. We have been unable to locate the missing device. The device may have contained your name, address, phone number, British Airways Employees Federal Credit Union (BAEFCU) credit card number, and Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: SkyOne Federal Credit Union
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266940.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-15	Harvey Mudd College / Ultimate Software	CA	3/22/2016	Electronic	Educational	Yes - Unknown #	Unknown

On March 4, 2016, several faculty and staff notified the Human Resources Office that they received an email message from Ultimate Software, the company that owns UltiPro payroll software, stating that their password for UltiPro had been changed. The unauthorized person accessed some faculty and staff records containing certain personal information, including name, address, Social Security number, and salary.

Attribution 1 Publication: MD AG's office Author:
Article Title: Harvey Mudd College
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266941.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-13	Mann Mortgage, Inc.	MT	3/25/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We are writing to you on behalf of our client, Mann Mortgage, Inc. ("Mann"), to notify you that Mann recently learned that certain Mann employees' work email accounts were compromised by a hacker using a phishing scam to gain access. The personal information contained in the accounts may have included names, addresses, Social Security numbers, and certain tax filing documentation relevant to their loan application.

Attribution 1 Publication: MD AG's office / MT AG's office Author:
Article Title: Mann Mortgage, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266961.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-12	Interstate Hotels & Resorts	VA	3/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 26, 2016 a PDF copy of your Form W-2, along with the Form W-2s of certain other individuals, was inadvertently sent in an e-mail to someone within Interstate who was not authorized to receive it. As you know, a Form W-2 contains the name, address and Social Security Number of an employee, among other things.

Attribution 1 Publication: MD AG's office Author:
Article Title: Interstate Hotels & Resorts
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266966.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-11	Lynn University	FL	2/19/2016	Electronic	Educational	Yes - Unknown #	Unknown

On January 19, 2016, it was brought to Lynn University's attention that the myLynn Student Finances page contained incorrect permission settings. The settings made it possible for information in the Refund Set-up portion to be viewable by individuals with Lynn University student log in credentials. Moreover, we can confirm that the only information that may have been viewable was students' names, student ID numbers, the dates of the requested refunds, the bank routing and account numbers where the refund was to be deposited, and the account types. No other personally identifiable information, such as Social Security numbers or credit card numbers, was viewable.

Attribution 1 Publication: MD AG's office Author:
Article Title: Lynn University
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266994.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 21 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-10	Applause App Quality, Inc.	MA	2/26/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 19, 2016, we became aware of a disclosure of certain Applause payroll data to an unauthorized party, as a result of a cyberattack. Unfortunately, a review of the data in question has determined that some of your personally identifiable information was acquired by this unauthorized party, including the following types of data: first name, last name, address, Social Security number, and 2015 salary.

Attribution 1 Publication: MD AG's office Author:
Article Title: Applause App Quality, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266995.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-09	Plano Synergy	IL	2/15/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 11, 2016, the Company experienced an incident that affected our systems. We became aware of the incident on the same day and commenced an immediate investigation. The information that was disclosed was a file containing employees' Form W-2 related information, which included the employee's name, address, social security number, wage and associated information from calendar year 2015, and information related to the Company.

Attribution 1 Publication: MD AG's office Author:
Article Title: Plano Synergy
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266996.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-08	Trop Gun Shop	PA	2/22/2016	Electronic	Business	Yes - Unknown #	Unknown

Trop Gun Shop learned on that, on or about January 10, 2016, malware was installed by unauthorized person(s) on portions of the Shop's website, including its online store. This resulted in a security breach that made certain personally-identifiable information accessible to those person(s)

Attribution 1 Publication: MD AG's office Author:
Article Title: Trop Gun Shop
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266997.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-07	VBrick Systems, Inc.	VA	4/22/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 24, 2016, Lisa Dias, an HR representative in VBrick's Wallingford, CT, office, received a "spoof" email that appeared to come from VBrick's CEO, Shelly Heiden, requesting copies of 2015 W-2 tax forms prepared for VBrick employees. Ms. Dias, believing this to be a genuine request, provided PDF copies of the 2015 W-2s of 141 of VBrick's current and past employees in response to the request.

Attribution 1 Publication: MD AG's office Author:
Article Title: VBrick Systems, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270376.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-06	Acceptance Insurance	TN	4/25/2016	Electronic	Business	Yes - Unknown #	Unknown

An Acceptance Insurance employee generated an electronic file containing the requested W-2 forms and sent the file as an attachment by e-mail to the former employee. After sending the message, the Acceptance Insurance employee discovered that the W-2 forms for other employees were inadvertently included.

Attribution 1 Publication: MD AG's office Author:
Article Title: Acceptance Insurance
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270378.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 22 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-05	O.C. Tanner	UT	4/26/2016	Electronic	Business	Yes - Unknown #	Unknown

On Thursday, April 14, 2016, O.C. Tanner was the targeted victim of an e-mail phishing attack. Through this attack, a request was made for employee 2015 Tax Form W-2 information. The 2015 Tax Form W -2 information was sent in response to the fraudulent email and included the following categories of information: (1) name; (2) address; (3) Social Security number; and (4) wage information, if any wages were earned from O.C. Tanner in 2015.

Attribution 1 Publication: NH AG's office, MD AG's office Author:
Article Title: O.C. Tanner
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/o-c-tanner-20160426.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-04	Oak Cliff Orthopaedic Associates	TX	12/16/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,057

On October 17, 2016, Oak Cliff Orthopaedic Associates discovered that boxes of old business records from the years 2006 and 2007 were stolen from their storage unit, but later discovered in a hotel room along with other stolen property.

Attribution 1 Publication: databreaches.net / hipaajournal.com / h Author:
Article Title: Oak Cliff Orthopaedic Associates Announce Incident Involving Theft of Business Records
Article URL: <https://www.databreaches.net/oak-cliff-orthopaedic-associates-announce-incident-involving-theft-of-business-records>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-03	Black Hawk College / Summit Reinsurance Services, Inc.	IL	12/16/2016	Electronic	Educational	Yes - Published #	1,000

Summit Reinsurance Services Inc. has notified the college that the names, Social Security numbers, health insurance information and medical records of 1,000 current and former employees could have been accessed after Summit's servers were infected, according to a BHC news release. The information also may have been compromised for these employees' dependents, according to BHC.

Attribution 1 Publication: qconline.com Author: Anthony Watt
Article Title: Security breach could affect BHC employees
Article URL: http://www.qconline.com/news/local/security-breach-could-affect-bhc-employees/article_582b0fd1-d353-5265-a3a1-f3b

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-02	Bleacher Report / Turner Broadcasting System	CA	12/16/2016	Electronic	Business	Yes - Unknown #	Unknown

On November 12, 2016, we became aware that an unauthorized party gained access to certain files containing limited Bleacher Report user information. We concluded that the unauthorized party may have acquired the first name, last name, username (email address), and password for Bleacher Report's website and mobile application user accounts. The Bleacher Report website and mobile application do not collect credit card numbers or other sensitive personal information, such as Social Security numbers.

Attribution 1 Publication: CA AG's office / databreaches.net Author:
Article Title: Bleacher Report / TBS
Article URL: https://oag.ca.gov/system/files/Bleacher%20Report%20Consumer%20Notice%20Redacted_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161216-01	Frederick County Public Schools	MD	12/13/2016	Electronic	Educational	Yes - Published #	1,000

Officials with Frederick County Public Schools say about 1,000 former students are affected by a pre-2010 data breach that was discovered in September. Schools spokesman Michael Raymond Doerrer said in an email Tuesday that students who attended county public schools between November 2005 and November 2006 were affected. He says the data includes names, Social Security number, and date of birth.

Attribution 1 Publication: WJLA.com Author:
Article Title: Public schools data breach affects 1,000 former students
Article URL: <http://wjla.com/news/local/public-schools-data-breach-affects-1000-former-students>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 23 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161215-06	Office of Dr. Melissa D. Selke	MD	12/14/2016	Electronic	Medical/Healthcare	Yes - Published #	4,277

On October 6, 2016, Princeton Medicine physician Dr. Melissa D. Selke discovered an unauthorized individual gained access to a server containing the electronic protected health information of more than 4,200 patients and used that access to install ransomware.

Attribution 1 Publication: databreaches.net / hhs.gov / NH AG's of Author:
Article Title: NJ family medicine practice notifying 4,277 patients after ransomware attack
Article URL: <https://www.databreaches.net/nj-family-medicine-practice-notifying-4277-patients-after-ransomware-attack/>

Attribution 2 Publication: hipaajournal.com Author:
Article Title: Princeton Medicine Ransomware Attack Reported
Article URL: <http://www.hipaajournal.com/princeton-medicine-ransomware-attack-reported-8609/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161215-05	K Partners Hotel Management	TX	4/2/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 2, 2016, we discovered that on that same day, as a result of a sophisticated network intrusion, an unauthorized third party gained access to an email account and a file server

Attribution 1 Publication: CA AG's office Author:
Article Title: K Partners Hotel Management
Article URL: <https://oag.ca.gov/system/files/K%20Partners%20-%20Notice%20Letter%20%5BRedacted%5D%20%286490516x7AB84>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161215-04	Office of Charles Stamitoles	FL	12/11/2016	Paper Data	Medical/Healthcare	Yes - Published #	5,600

Charles Stamitoles FL Healthcare Provider 5600 12/11/2016 Improper Disposal Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Charles Stamitoles
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161215-03	CHI Franciscan Health Hospice - Tacoma	WA	11/28/2016	Electronic	Medical/Healthcare	Yes - Published #	12,413

On October 18, 2016 an employee with Franciscan Hospice- Tacoma had her backpack stolen when a thief smashed the window of her locked car and accessed the vehicle. The backpack contained a CHI Franciscan issued laptop, mobile phone, paper documents with patient information, as well as a personal day planner that contained the staff member's username and passwords for computer and medical record access. The files located on the laptop may have included patient electronic medical record treatment information, name, address, phone number, social security number, insurance number, and next of kin name and contact information of 1,223 Washington residents.

Attribution 1 Publication: hhs.gov / WA AG's office Author:
Article Title: CHI Franciscan Health Hospice - Tacoma
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161215-02	Appalachian Gastroenterology, P.A.	NC	12/10/2016	Electronic	Medical/Healthcare	Yes - Published #	11,000

Appalachian Gastroenterology, P.A. NC Healthcare Provider 11000 12/10/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Appalachian Gastroenterology, P.A.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 24 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161215-01	Yahoo #2	CA	12/16/2016	Electronic	Business	Yes - Unknown #	Unknown

Yahoo, already reeling from its September disclosure that 500 million user accounts had been hacked in 2014, disclosed Wednesday that a different attack in 2013 compromised more than 1 billion accounts.

Attribution 1 Publication: nytimes.com Author:
 Article Title: Yahoo Says 1 Billion User Accounts Were Hacked
 Article URL: http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=1

Attribution 2 Publication: krebsonsecurity.com Author:
 Article Title: My Yahoo Account Was Hacked! Now What?
 Article URL: <https://krebsonsecurity.com/2016/12/my-yahoo-account-was-hacked-now-what/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161213-02	BraceAbility	IA	9/24/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 28, 2016, BraceAbility, Inc. learned of a possible security incident involving its online ordering website. We immediately engaged independent IT forensic experts to assist with our investigation. The information potentially exposed includes your name, address, card number, verification code, and/or the card's expiration date as well as information related to your online purchase.

Attribution 1 Publication: CA AG's office / MT AG's office Author:
 Article Title: BraceAbility
 Article URL: https://oag.ca.gov/system/files/BraceAbility%20notice%20only%20_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161213-01	Quest Diagnostics	NJ	12/12/2016	Electronic	Medical/Healthcare	Yes - Published #	34,055

On November 26th an unauthorized third party accessed the MyQuest by Care360® internet application and obtained PHI of approximately 34,000 patients. The data included name, date of birth, lab results, and, in some instances, telephone numbers.

Attribution 1 Publication: CA AG's office / databreaches.net / OR Author:
 Article Title: Quest Diagnostics
 Article URL: https://oag.ca.gov/system/files/Patient%20Notice%20FINAL_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-13	University of Wisconsin - Madison	WI	12/9/2016	Electronic	Educational	Yes - Published #	1,123

On Nov. 3, university officials discovered that a hacker had gained unauthorized access to the University of Wisconsin Law School's server earlier that day. Upon discovery of the breach, UW-Madison removed the affected records from the hacked server and contacted law enforcement authorities. The database contained applicants' Social Security numbers, which were paired with corresponding names. No other personal data was accessed, according to UW-Madison.

Attribution 1 Publication: scmagazine.com Author:
 Article Title: University of Wisconsin-Madison data breach impacts 1000-plus former law school applicants
 Article URL: <https://www.scmagazine.com/university-of-wisconsin-madison-data-breach-impacts-1000-plus-former-law-school-app/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-12	FriendFinders Network	CA	11/14/2016	Electronic	Business	Yes - Unknown #	Unknown

A hack against popular adult dating and entertainment company FriendFinder Networks exposed data related to more than 412 million user accounts, according to a report from breach notification site LeakedSource.

Attribution 1 Publication: washingtonpost.com / CA AG's office Author:
 Article Title: Adult FriendFinder hit with one of the biggest data breaches ever, report says
 Article URL: <https://www.washingtonpost.com/news/the-switch/wp/2016/11/14/adult-friendfinder-hit-with-one-of-the-biggest-data-b/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-11	PhyMed	TN	4/29/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On April 18 and April 19, 2016, in response to what appeared to the employee to be a legitimate requests for such information from PhyMed's CEO, the employee sent outside the company approximately six .pdf files containing 2015 IRS W-2 payroll information related to PhyMed current and former employees who received a 2015 IRS W-2 form.

Attribution 1 Publication: MD AG's office Author:
Article Title: PhyMed
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270392.pdf - search=PhyMed%20>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-10	Total Community Options, Inc. dba InnovAge	CO	5/2/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 22, 2016, Innov Age discovered that its was targeted in an email spoofing attack. Through this attack, what was then believed to be a legitimate request was made on April 8, 2016 for 2015 IRS Tax Form W-2 information.

Attribution 1 Publication: MD AG's office / MT AG's office Author:
Article Title: Total Community Options, Inc. dba InnovAge
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270395.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-09	Raging Wire Data Centers	NV	5/5/2016	Electronic	Business	Yes - Unknown #	Unknown

An unauthorized individual impersonating a RagingWire executive sent a fraudulent email on February 23, 2016, to RagingWire requesting the W-2 information of RagingWire employees. RagingWire responded to the request and sent a file to the impersonator.

Attribution 1 Publication: MD AG's office Author:
Article Title: Raging Wire Data Centers
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270403.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-08	Veterans Management Services, Inc.	VA	4/25/2016	Electronic	Business	Yes - Unknown #	Unknown

VMSI discovered a phishing incident occurred on March 10, 2016 in which your 2015 W-2 Wage and Tax Statement was inadvertently disclosed when fulfilling what was believed to be a legitimate request for information. It is with sincere regret that we must notify you that you are an individual potentially affected by this breach. The information compromised included your W-2 containing your full name, mailing address, and Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Veterans Management Services, Inc.
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270380%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270380%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-07	Avinger, Inc.	CA	4/26/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 21, 2016, an Avinger employee was tricked into disclosing employees' W-2 information to an unauthorized individual as part of a phishing attack. Avinger discovered the disclosure on April 22, 2016. The information included employees' names, addresses, social security numbers, wages, and withholdings.

Attribution 1 Publication: MD AG's office Author:
Article Title: Avinger, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270382.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-06	Symphony EYC	MA	4/28/2016	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you that an unauthorized acquisition of your personal information occurred on April 27, 2016 in the form of W2 statements for 2015.

Attribution 1 Publication: MD AG's office Author:
Article Title: Symphony EYC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270385.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-05	Group Benefit Services	MD	5/9/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 8, 2016, GBS learned of a programming error in a software upgrade (installed the afternoon of February 5, 2016) for an online benefits portal GBS provides to one of its clients. The upgrade was intended to allow the client's employees to access their online benefit transaction history. However, due to the error, if any of the client's employees clicked on the link to view their transaction history and then clicked on the back button, a link was available that could have permitted the user to view other employees' transaction history.

Attribution 1 Publication: MD AGs office / MT AG's office Author:
Article Title: Group Benefit Services
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270409.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-04	Astreya Partners, Inc.	CA	5/6/2016	Electronic	Business	Yes - Unknown #	Unknown

Astreya learned on May 2, 2016 that Form W-2 Wage and Tax Statements of employees had been acquired without authorization. It appears that information of one (1) Maryland resident was accessed without authorization. The W-2 information included names, addresses, Social Security numbers and tax information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Astreya Partners, Inc.
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270411%20\(1\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270411%20(1).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-03	Westcor Land Title Insurance Company	FL	5/10/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to notify you that on April 28, 2016, Westcor Land Title Insurance Company, determined that it had been the victim of an email phishing scheme, occurring on that same day, which may have resulted in an unauthorized person or entity obtaining a copy of employee 2015 W-2 forms.

Attribution 1 Publication: MD AG's office Author:
Article Title: Westcor Land Title Insurance Company
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270413.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-02	BlackHeart Records	NY	5/12/2016	Electronic	Business	Yes - Unknown #	Unknown

On Dec 1st the MacKeeper Security Research Center discovered Joan Jett's BlackHeart Records leaking hundreds of gigabytes of data online. BlackHeart Records is an Independent label founded by Joan Jett and Kenny Laguna and has a good reputation as an established label with a range of well known artists. The data breach is a massive treasure trove for fans and cyber criminals alike. There are unreleased tracks, never before seen pictures, even rejection letters from 1980 when Joan Jett was trying to get a record deal. There are also social security numbers of label employees and band members, internal memos and scanned checks of royalty payments and much more.

Attribution 1 Publication: databreaches.net Author:
Article Title: BlackHeart Records
Article URL: <https://mackeeper.com/blog/post/307-joan-jetts-blackheart-records-leaks-thousands-of-files-online>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 27 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161212-01	Anchor Loans	CA	11/7/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On or about November 7, 2016, a security researcher accessed one of our databases that was publicly exposed on the Internet. We reacted swiftly by reconfiguring the database and moving to secure the data. Because the security researcher had access to this database, your personal information may have been exposed.

Attribution 1 Publication: CA AG's office / NH AG's office / VT AG' Author:
Article Title: Anchor Loans
Article URL: https://oag.ca.gov/system/files/Anchor%20Loans%20Sample%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161209-08	Henry County	GA	12/7/2016	Electronic	Government/Military	Yes - Published #	17,841

The county last week sent a letter to 17,841 voters to notify them of the computer hacking incident that occurred Oct. 31. County officials also offered a free year of service from a credit-monitoring company. With each name in the file of voter registrations was the person's address, phone number, ZIP code, party affiliation, the last four digits of their Social Security number, and their driver's license number.

Attribution 1 Publication: toledoblade.com / databreaches.net Author:
Article Title: Residents' information is exposed in hacking
Article URL: <http://www.toledoblade.com/Politics/2016/12/07/Residents-information-is-exposed-in-Henry-County-hacking.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161209-07	University of Vermont	VT	11/30/2016	Electronic	Educational	Yes - Unknown #	Unknown

UVM's Information Security Team received a report on September 15,2016 that a purse owned by a UVM employee was stolen. The purse contained a USB drive that contained your personally identifiable information. 1. A scanned copy of UVM's Disclosure Notice. The Disclosure Notice contains your full name (first, last and middle), social security number and date of birth. 2. A scanned copy of UVM's Acknowledgment and Authorization for consumer reports. The Acknowledgment and Authorization form includes your name, social security number, date of birth, aliases, driver's license number, driver's license state of issuance, phone number, email address, present address and previous addresses.

Attribution 1 Publication: VT AG's office / databreaches.net Author:
Article Title: University of Vermont
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/University%20of%20Vermont%20SBN%20to%20Consu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161209-06	Citrix Systems	FL	12/6/2016	Electronic	Business	Yes - Unknown #	Unknown

The breach involved an unknown and unauthorized person accessing and downloading client files saved on an online Citrix ShareFile server. The information accessed by the unauthorized person primarily includes QuickBooks files and summary statements of tax returns. More specifically, some of the information accessed includes client names, social security numbers, personal tax identification numbers, and mailing addresses. I am unsure at this time whether the information as accessed was encrypted on Citrix's server such that the data is unreadable, so I am giving this notice out of an abundance of caution.

Attribution 1 Publication: MT AG's office Author:
Article Title: Citrix Systems
Article URL: <https://dojmt.gov/wp-content/uploads/Citrix-Systems-1.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161209-05	Young Adult Institute, Inc.	NY	11/28/2016	Electronic	Medical/Healthcare	Yes - Published #	913

Young Adult Institute, Inc. NY Healthcare Provider 913 11/28/2016 Theft Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: Young Adult Institute, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 28 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161209-04	UnitedHealth Group Single Affiliated Covered Entity #2	MN	11/22/2016	Electronic	Medical/Healthcare	Yes - Published #	1,408
UnitedHealth Group Single Affiliated Covered Entity MN Health Plan 1408 11/22/2016 Unauthorized Access/Disclosure Other							

Attribution 1 Publication: hhs.gov Author:
 Article Title: UnitedHealth Group Single Affiliated Covered Entity #2
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161209-03	Preventice Services, LLC	TX	12/7/2016	Electronic	Medical/Healthcare	Yes - Published #	6,800
Preventice Services, LLC TX Healthcare Provider 6800 12/07/2016 Unauthorized Access/Disclosure Other							

Attribution 1 Publication: hhs.gov Author:
 Article Title: Preventice Services, LLC
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=6774A1EF96B5EB6CE841CC558824E10A

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161209-02	CVS Health	RI	12/5/2016	Electronic	Medical/Healthcare	Yes - Published #	626
CVS Health RI Healthcare Provider 626 12/05/2016 Theft Paper/							

Attribution 1 Publication: hhs.gov Author:
 Article Title: CVS Health
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161209-01	Managed Health Services #2	IN	11/29/2016	Electronic	Medical/Healthcare	Yes - Published #	5,500
Managed Health Services IN Health Plan 5500 11/29/2016 Theft Email, Laptop							

Attribution 1 Publication: Author:
 Article Title: Managed Health Services #2
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=D3F46C7984D850963A2AF0F4A86EAE99

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161208-01	East Valley Community Health Center	CA	12/14/2016	Electronic	Medical/Healthcare	Yes - Published #	65,000

We learned that your personal information, including name, date of birth, address, medical record number, health diagnosis codes and insurance account number may have been compromised. However, information such as social security number and/or CA identification/driver license number was not included. On October 18th, an unknown individual logged into an EVCHC server without authorization and installed Troldesh/Shade, encrypting (locking) the files that were stored on the server, this is also known as a ransomware attack. One of the files that was encrypted had patient health information on it, which came from claims that were submitted to health plans. However, to date, there is no indication that the information has been accessed or used by the unauthorized individual.

Attribution 1 Publication: CA AG's office / hipaajournal.com / hhs. Author:
 Article Title: East Valley Community Health Center
 Article URL: https://oag.ca.gov/system/files/Patient%20Breach%20Notification%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-11	Wisconsin National Guard Association	WI	11/28/2016	Electronic	Business	Yes - Unknown #	Unknown

Recently, we became aware of an unauthorized intrusion into a database used by the Wisconsin National Guard Association (WINGA) in connection with their group life insurance program. New York Life Insurance Company is the insurer for the program. This intrusion may have resulted in unauthorized access to the personal information of individuals and beneficiaries currently or previously insured under the WINGA group life insurance program, including the name, address, date of birth, and social security number of 1 New Hampshire resident.

Attribution 1 Publication: Nh AG's office Author:
Article Title: Wisconsin National Guard Association
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/winga-20161123.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-10	Educents	CA	11/22/2016	Electronic	Business	Yes - Unknown #	Unknown

Specifically, between September 26, 2016 and October 18, 2016, an unauthorized person may have gained access to credit card numbers and other information that certain Educents customers entered during the Educents checkout process.

Attribution 1 Publication: NH AG's office Author:
Article Title: Educents
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/educents-20161122.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-09	Caesars Entertainment	NV	11/25/2016	Paper Data	Business	Yes - Unknown #	Unknown

On or around November 8, 2016, Caesars learned that the Las Vegas Metropolitan Police Department ("LVMPD") had discovered hard copies of customer credit applications and other paper customer records in the possession of a suspect in an unrelated investigation. Through its own recent review, Caesars determined that most of these records were likely stolen from a storage facility in one of its properties on or around July 29, 2015. The records found by the LVMPD varied from individual to individual but included some or all of the following: name, residence and business addresses, email address, telephone numbers, date of birth, Social Security number, driver's license number, employment information and bank account information (although no PINs or passwords). Additionally, in some instances, the records also may have included photocopies of customers' driver licenses or similar identification documents.

Attribution 1 Publication: NH AG's office Author:
Article Title: Caesars Entertainment
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/caesars-20161128.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-08	Brennan Recupero Cascione Scungio and McAllister LLP	RI	11/22/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 15, 2016, the credentials for a Brennan Recupero attorney were briefly used by an unauthorized individual to remotely access its computer network.

Attribution 1 Publication: Author:
Article Title: Brennan Recupero Cascione Scungio and McAllister LLP
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/brennan-recupero-20161122.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-07	BWTX Associates	TX	11/21/2016	Electronic	Business	Yes - Unknown #	Unknown

BWTX recently began investigating unusual activity reported by its credit card processor. Leading third party forensic experts were retained to assist BWTX with this investigation and to determine what happened and who may be impacted. On or around September 15, 2016, malicious files were identified on a BWTX device used to process payment information for guests' hotel bookings,

Attribution 1 Publication: NH AG's office Author:
Article Title: BWTX Associates
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/bwtx-20161121.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-06	SwervePoint, LLC	MA	11/29/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 6, 2016, SwervePoint discovered that an unidentified third party had injected malicious code into its e-commerce platform used on the <<CLIENT>>. The malicious code enabled the unidentified third party to acquire credit card information while the purchase took place.

Attribution 1 Publication: MT AG's office / NH AG's office Author:
Article Title: SwervePoint, LLC
Article URL: <https://dojmt.gov/wp-content/uploads/Swervepoint.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-05	Baylor College of Medicine	TX	11/30/2016	Electronic	Educational	Yes - Unknown #	Unknown

In late October, Baylor College of Medicine discovered that a database containing information about applicants to the school may have been compromised, and immediately began investigating. The information involved included first name, middle initial, last name, and Social Security number of individuals who submitted applications to Baylor College of Medicine. It is likely that there was unauthorized access to this information.

Attribution 1 Publication: MT AG's office / NH AG's office Author:
Article Title: Baylor College of Medicine
Article URL: <https://dojmt.gov/wp-content/uploads/Baylor-College-of-Medicine.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-04	Guilmartin, DiPiro & Sokolowski, LLC	CT	12/2/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 17, 2016 one of GDS' software partners informed GDS that it had detected a fraudulent electronic tax return filing related to one of GDS' clients. On November 2, 2016, the computer forensic company informed GDS that it appeared that an unauthorized user had gained access to a GDS server and may have accessed files containing your personal information. These files contained information related to your tax return including your name, address, Social Security number, wage information, and possibly your bank account information.

Attribution 1 Publication: VT AG's office / MT AG's office / NH AG' Author:
Article Title: Guilmartin, DiPiro & Sokolowski, LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Guilmartin%20DiPiro%20and%20Sokolowski%20LLC%

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-03	Cleveland Clinic Akron General / Ambucor	OH	11/25/2016	Electronic	Medical/Healthcare	Yes - Published #	730

A company that contracts with Cleveland Clinic Akron General to provide remote monitoring services to patients notified 730 Akron General patients this week that their protected health information may have been compromised. According to the company, Ambucor, a former employee improperly downloaded confidential company information onto portable USB drives, commonly known as "thumb" or "flash" drives.

Attribution 1 Publication: ohio.com Author:
Article Title: Cleveland Clinic Akron General / Ambucor
Article URL: <http://www.ohio.com/news/local/regional-news-briefs-nov-26-1.729739>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-02	New Mexico Heart Institute / Ambucor	NM	11/25/2016	Electronic	Medical/Healthcare	Yes - Published #	4,185

The New Mexico Heart Institute this week reported a privacy breach at one of its vendors, affecting more than 4,000 patients. (Ambucor)

Attribution 1 Publication: abqjournal.com / hhs.com Author:
Article Title: Heart Institute reports privacy breach
Article URL: <https://www.abqjournal.com/895989/heart-institute-reports-privacy-breach.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161206-01	Glendale Adventist Medical Center / White Memorial	CA	12/3/2016	Electronic	Medical/Healthcare	Yes - Published #	528

Glendale Adventist officials said in a statement on Friday that the protected health information of 528 patients was accessed without authorization by a hospital employee. The unauthorized access included 88 patient records from Glendale Adventist's sister hospital, White Memorial Medical Center in Boyle Heights.

Attribution 1 Publication: latimes.com / databreaches.net / becker Author:
Article Title: <http://www.latimes.com/socal/glendale-news-press/news/tn-gnp-me-privacy-breach-20161202-story.html>
Article URL: <http://www.latimes.com/socal/glendale-news-press/news/tn-gnp-me-privacy-breach-20161202-story.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-13	TSYS Merchant Solutions	NE	11/29/2016	Electronic	Business	Yes - Unknown #	Unknown

On November 14, 2016, the TIN Mismatch file that included your information was sent to the ISO that processes your transactions. A representative of a TSYS partner bank was inadvertently copied on the email. The result of this error was that your merchant information was accessible to this bank representative.

Attribution 1 Publication: CA AG's office Author:
Article Title: TSYS Merchant Solutions
Article URL: https://oag.ca.gov/system/files/TSYS%20Merchant%20Data%20Breach%20Notification_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-12	San Jose Evergreen Community College District	CA	12/1/2016	Electronic	Educational	Yes - Unknown #	Unknown

On November 7, 2016, we learned that an SJECCD employee had inadvertently uploaded a file containing the personal information of certain SJECCD students to a publicly accessible folder on the SJECCD website. The personal information contained in the file may have included your name, date of birth, and Social Security number.

Attribution 1 Publication: CA AG's office / databreaches.net / MT Author:
Article Title: San Jose Evergreen Community College District
Article URL: <https://oag.ca.gov/system/files/San%20Jose%20Evergreen%20Community%20College%20District%20Security%20Inci>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-11	LANG Companies	WI	9/1/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 12, 2016, we learned that unauthorized individuals installed malicious software on the computer server used to process credit card transactions at www.LANG.com. Based on our investigation, we believe that customers who placed an order on our website from September 1, 2016 to October 19, 2016, may have had information associated with the order transmitted outside of our system.

Attribution 1 Publication: CA AG's office / VT AG's office / MT AG' Author:
Article Title: LANG Companies
Article URL: https://oag.ca.gov/system/files/CA%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-10	Office of Hillary Tentler	CA	11/4/2016	Electronic	Business	Yes - Unknown #	Unknown

On November 4, 2016, I discovered that my home was broken into earlier in that day. Upon discovery, I immediately notified the Santa Barbara County Sheriff's office and a police report was filed. Unfortunately, along with personal effects, the burglars stole three back up hard drives for my practice.

Attribution 1 Publication: CA AG's office Author:
Article Title: Office of Hillary Tentler
Article URL: https://oag.ca.gov/system/files/Tentler%20Letter%20Version%201_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 32 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-09	Vision Care Florida	FL	11/16/2016	Electronic	Medical/Healthcare	Yes - Published #	7,500

Vision Care Florida, LLC FL Healthcare Provider 7500 11/16/2016 Unauthorized Access/Disclosure Desktop Computer

Attribution 1 Publication: [hhs.gov](#) Author:
Article Title: Vision Care Florida
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-08	OptumHealth New Mexico	MN	11/18/2016	Electronic	Medical/Healthcare	Yes - Published #	2,006

On Nov. 17, OptumHealth New Mexico began notifying members that a flash drive, mailed by an unnamed vendor on September 16, was discovered on September 26 to have been lost in the postal mail. From their FAQ on the incident:

Attribution 1 Publication: [hhs.gov / databreaches.net](#) Author:
Article Title: OptumHealth New Mexico notifies 2,006 members of breach
Article URL: <https://www.databreaches.net/optumhealth-new-mexico-notifies-2006-members-of-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-07	Louisiana Health Cooperative, Inc.	LA	11/30/2016	Electronic	Medical/Healthcare	Yes - Published #	8,000

Louisiana Health Cooperative, Inc. in Rehabilitation LA Health Plan 8000 11/30/2016 Hacking/IT Incident Other

Attribution 1 Publication: [hhs.gov](#) Author:
Article Title: Louisiana Health Cooperative, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-06	Sagewood / LCS Westminster Partnership	AZ	11/22/2016	Electronic	Medical/Healthcare	Yes - Published #	863

On Sept. 29, 2016, Sagewood discovered that the ransomware attack may have gained unauthorized access to employee and resident information as well as health insurance claim information. The resident and health insurance information may have included names, addresses, dates of birth, phone numbers, social security numbers, and possibly Medicare numbers or national identification numbers.

Attribution 1 Publication: [hhs.gov / databreaches.net / hipaaajournal](#) Author:
Article Title: Sagewood / LCS Westminister Partnership
Article URL: <https://www.databreaches.net/sagewood-notifies-863-employees-and-residents-of-cyber-attack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-05	Camas Center Clinic / Kalispel Tribe of Indians	WA	11/21/2016	Electronic	Medical/Healthcare	Yes - Published #	504

Camas Center Clinic, Kalispel Tribe of Indians WA Healthcare Provider 504 11/21/2016 Unauthorized Access/Disclosure Desktop Computer, Paper/Films

Attribution 1 Publication: [hhs.gov](#) Author:
Article Title: Camas Center Clinic / Kalispel Tribe of Indians
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-04	Berkshire Medical Center / Ambucor	MA	11/23/2016	Electronic	Medical/Healthcare	Yes - Published #	1,745

Personal information on hundreds of Berkshire Medical Center cardiology patients have been found on thumb drives recovered from a former employee of an outside service vendor, the hospital reported on Wednesday.

Attribution 1 Publication: TheBerkshireEagle.com / beckershospit Author:
Article Title: Hundreds of BMC patients' info found on vendor's thumb drives
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-03	Akron General Medical Center	OH	11/23/2016	Electronic	Medical/Healthcare	Yes - Published #	730

Akron General Medical Center OH Healthcare Provider 730 11/23/2016 Unauthorized Access/Disclosure Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: Akron General Medical Center
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-02	Group Health Incorporated	NY	11/22/2016	Paper Data	Medical/Healthcare	Yes - Published #	81,112

Group Health Incorporated NY Health Plan 81122 11/22/2016 Unauthorized Access/Disclosure Network Server, Other, Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Group Health Incorporated
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161205-01	Chesapeake Public Schools	VA	12/3/2016	Electronic	Educational	Yes - Published #	10,827

Chesapeake Public Schools are warning employees about a possible data breach after an employee's laptop was stolen.

Kellie Goral with CPS says that the laptop was password protected and there is currently no information that data breach has affected anyone. The personal information on the files included names, social security numbers, and bank account numbers of some present and past employees.

CPS has notified over 10,000 people that could be affected and have setup a free protective service.

Attribution 1 Publication: WAVY.com Author:
Article Title: Chesapeake Public Schools warn about data breach
Article URL: <http://wavy.com/2016/12/03/chesapeake-public-schools-warn-about-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161202-01	BLU	FL	11/25/2016	Electronic	Business	Yes - Published #	120,000

Earlier this month, the Californian consumer electronics manufacturer admitted to a significant security breach which affected approximately 120,000 of its active devices. An app called "Wireless Update" has been collecting personal data from some BLU customers including text messages, call logs, and contact lists without any authorization and forwarded them to a private Chinese server.

Attribution 1 Publication: androidheadlines.com Author:
Article Title: BLU Faces Possible Class Action Lawsuit Over Security Breach
Article URL: <http://www.androidheadlines.com/2016/11/blu-faces-possible-class-action-lawsuit-over-security-breach.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-10	U.S. Olympic Committee	CO	11/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On November 18, 2016, the USOC learned that an unauthorized individual had gained access to an email sent to a government contractor who performed security clearances in advance of a USOC event. The email attachment contained certain personal information, including name, address, date of birth, telephone number, social security number and passport information for a limited number of individuals. Based on its investigation to date, the USOC has not identified any evidence that this incident involves any unauthorized access to or use of any usoc computer systems or networks.

Attribution 1 Publication: NH AG's office / databreaches.net Author:
 Article Title: United States Olympic Committee
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/usoc-20161121.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-09	IDEO.org	CA	11/9/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 30, 2016, a work laptop was stolen from an employee's home. The laptop contained personal information that included social security numbers, driver's license numbers, and passport numbers.

Attribution 1 Publication: NH AG's office Author:
 Article Title: IDEO.org
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/ideo-org-20161109.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-08	State Street Corporation	MA	11/28/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On July 16, 2016, one of our vendors transferred information about certain State Street accounts to a United States-based bank as part of a movement of accounts between financial institutions. During the transfer, because of a software programming error, your information was inadvertently included among the records sent to the other bank. Specifically, the personal information that was inadvertently shared with the other bank included name, Social Security and/or taxpayer ID number, date of birth, address, phone number, and email address information.

Attribution 1 Publication: MT AG's office / NH AG's office Author:
 Article Title: State Street Corporation
 Article URL: <https://dojmt.gov/wp-content/uploads/State-Street.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-07	Aon Hewitt	IL	7/7/2016	Electronic	Business	Yes - Published #	2,892

We are writing to notify you of an incident that occurred on or around July 2016 that involved the potential, unauthorized access to your personal information. The personal information potentially accessed by the unknown third person or persons was limited to your first and last name, social security number, saved contact information (such as mailing address or phone numbers), date of birth, beneficiary information, employee ID number, employment status, and health care plan status.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Aon Hewitt
 Article URL: https://oag.ca.gov/system/files/Ppt%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-06	Consultants in Neurological Surgery, LLP	FL	11/8/2016	Paper Data	Medical/Healthcare	Yes - Published #	800

Consultants in Neurological Surgery, LLP FL Healthcare Provider 800 11/08/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: Consultants in Neurological Surgery, LLP
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-05	Pinellas County Board of County Commissioners	FL	11/18/2016	Electronic	Government/Military	Yes - Published #	2,800

Pinellas County Board of County Commissioners FL Health Plan 2800 11/18/2016 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: Pinellas County Board of County Commissioners
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 35 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-04	Lister Healthcare	AL	11/9/2016	Electronic	Medical/Healthcare	Yes - Published #	1,349

Lister Healthcare AL Healthcare Provider 1349 11/09/2016 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Lister Healthcare
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-03	North Texas Heart Center, P.A.	TX	11/21/2016	Electronic	Medical/Healthcare	Yes - Published #	4,210

North Texas Heart Center, P.A. TX Healthcare Provider 4210 11/21/2016 Theft Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: North Texas Heart Center, P.A.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-02	Darlingten	GA	11/22/2016	Electronic	Medical/Healthcare	Yes - Published #	600

Darlingten GA Business Associate 600 11/22/2016 Improper Disposal Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Darlingten
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161129-01	Spreadshirt.com	MA	11/7/2016	Electronic	Business	Yes - Unknown #	Unknown

An unauthorized user with a list of usernames and passwords obtained from a past hack of major websites has used that list to attempt to log in to different websites, including Spreadshirt.com, hoping that users had the same usernames and passwords across many different websites. Spreadshirt believes this unauthorized user logged into your account using your credentials.

Attribution 1 Publication: VT AG's office Author:
Article Title: Spreadshirt.com USA
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Spreadshirt.%20Inc.%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-21	AdultFriendFinder	CA	11/13/2016	Electronic	Business	Yes - Unknown #	Unknown

A massive data breach targeting adult dating and entertainment company Friend Finder Network has exposed more than 412 million accounts. The hack includes 339 million accounts from AdultFriendFinder.com, which the company describes as the "world's largest sex and swinger community."

Attribution 1 Publication: zdnet.com Author:
Article Title: AdultFriendFinder network hack exposes 412 million accounts
Article URL: <http://www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-20	City of Plummer	ID	9/9/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

On April 14, 2016, the City's computer systems were infected with a ransomware virus. We began an investigation to determine what happened and to determine whether any sensitive information was accessed or acquired. The following types of your information may have been located on the server: your name, <<driver's license number, credit card information, date of birth, bank account information, Tribal ID number, and Social Security number.

Attribution 1 Publication: MT AG's office Author:
 Article Title: City of Plummer
 Article URL: <https://dojmt.gov/wp-content/uploads/City-of-Plummer.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-19	Capital One	VA	9/15/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

A former employee at a Capital One® service provider, while still working on Capital One matters, accessed it when they shouldn't have, potentially for illicit purposes. While we do not see any suspicious account transactions related to this, please keep an eye out for unauthorized transactions (including outside of Capital One) because the person saw your account information, such as your name, account number, and social security number.

Attribution 1 Publication: MT AG's office Author:
 Article Title: Capital One
 Article URL: <https://dojmt.gov/wp-content/uploads/Capital-One.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-18	Boeing Employees Credit Union	WA	9/26/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On or around August 9, 2016, we detected suspicious activity in your BECU Online Banking service and upon investigation, determined that unauthorized individuals were able to obtain access to your account by utilizing a username and password that we believe they obtained from infiltrating a non-BECU website.

Attribution 1 Publication: MT AG's office Author:
 Article Title: Boeing Employees Credit Union
 Article URL: <https://dojmt.gov/wp-content/uploads/BECU.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-17	Office of Dale A. Wein, Prof. LLC	SD	10/1/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 12, 2016, we discovered that as a result of a sophisticated network intrusion between late May 2016 and July 12, 2016, an unauthorized third party gained access to one of our servers. Upon learning of the issue, our incident response team promptly launched an investigation and notified the U.S. Trustee's Office and law enforcement. Because we value our relationship with you, we wanted to make you aware of this incident because the unauthorized party may have accessed some of your personal information with in the Infected server, including your full name and Social Security number.

Attribution 1 Publication: MT AG's office Author:
 Article Title: Office of Dale A. Wein, Prof. LLC
 Article URL: <https://dojmt.gov/wp-content/uploads/Dale-A-Wein-Prof-LLC.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-16	University of Montana	MT	10/6/2016	Electronic	Educational	Yes - Unknown #	Unknown

We are contacting you regarding an information security incident that occurred on September 12, 2016, at the University of Montana. In this incident, an attacker fraudulently obtained the email credentials of an employee of the ASUM Day care. The incident was discovered on September 14, 2016, when the .attacker. used the account to send out large amounts of spam. UM took inunediate action and disabled the email account. A thorough forensic investigation revealed that the attacker gained access to an email which contained a single cell phone photo of your social security card.

Attribution 1 Publication: MT AG's office Author:
 Article Title: University of Montana
 Article URL: <https://dojmt.gov/wp-content/uploads/University-of-Montana.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 37 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-15	Natural Life Collections, Inc.	FL	10/20/2016	Electronic	Business	Yes - Unknown #	Unknown

The compromise of our eCommerce checkout page occurred on September 18, 2016 and may impact the security of credit cards customers used for purchases through our site, naturallife.com, from September 18, 2016 to September 23, 2016. Based on our investigation, we can confirm that the information potentially involved in this incident may have included your name, billing and shipping address, credit card number, card expiration date and CVV (3 or 4 digit code on the front or back of the card). It is also possible that your email address and password you use to make purchases through naturallife.com was involved.

Attribution 1 Publication: MT AG's office Author:
Article Title: Natural Life Collections, Inc.
Article URL: <https://dojmt.gov/wp-content/uploads/Natural-Life-Collections.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-14	National Satellite Center	CA	10/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 13, 2016, we discovered that a former employee was able to gain access to a current employee's computer and to those files the current employee has access. We immediately conducted an investigation and determined that the files that former employee may have accessed may have contained your name, address, date of birth, and Social Security number. Law enforcement has been notified and we are cooperating with their investigation.

Attribution 1 Publication: MT AG's office Author:
Article Title: National Satellite Center
Article URL: <https://dojmt.gov/wp-content/uploads/Pacific-Concepts-Group-dba-National-Satellite-Center.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-13	Christian Louboutin	NY	11/3/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 28, 2016, unknown individuals gained access to our U.S. online boutique, through unauthorized use of an administrative password from a third party website manager. Unfortunately, and despite all the security measures implemented on the website, the intruders were able to access information associated with online purchases through this website between August 28, 2016 and October 3, 2016.

Attribution 1 Publication: MT AG's office Author:
Article Title: Christian Louboutin
Article URL: <https://dojmt.gov/wp-content/uploads/Christian-Louboutin.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-12	Baker, Overby & Moore, Inc., P.S.	WA	11/8/2016	Electronic	Business	Yes - Unknown #	Unknown

During the weekend of October 8th and 9th, 2016, a burglar broke into our locked Forks, Washington office and stole a laptop computer that contained client personal information. The following information may have been involved: passport number, name and Social Security number.

Attribution 1 Publication: MT AG's office Author:
Article Title: Baker, Overby & Moore, Inc., P.S.
Article URL: <https://dojmt.gov/wp-content/uploads/Baker-Overby-Moore-Inc.-P.S..pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-11	State Farm	IL	10/20/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 27, 2016, State Farm became aware that unauthorized online access to some customers' accounts on statefarm.com had occurred. We initiated an investigation to determine the extent of the unauthorized activity. Our investigation indicates that someone with information about you was able to register and/or access your State Farm accounts online at statefarm.com. Further, our investigation has identified that in some cases, unauthorized transactions and/or customer profile changes may have been processed. Other personal information may have also been accessed.

Attribution 1 Publication: MT AG's office Author:
Article Title: State Farm
Article URL: <https://dojmt.gov/wp-content/uploads/State-Farm-Mutual-Automobile-Insurance-Company.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-10	Yummie by Heather Thomson	NY	11/16/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to inform you of a data security incident that we have just uncovered, which involved your personal information. Between October 4, 2016 and November 1, 2016, malicious "credit card skimming" software was installed by an unauthorized foreign party on the front end of our website, www.yummie.com, without our knowledge or consent. Consequently, when you recently made a purchase from our website, your personal data was illegally diverted, including your name, billing address, credit card number, expiration date and card security/access code, and your user name and password.

Attribution 1 Publication: MT AG's office / NH AG's office Author:
Article Title: Yummie by Heather Thomson
Article URL: <https://dojmt.gov/wp-content/uploads/Yummie.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-09	Ameriprise Financial	MN	11/18/2016	Paper Data	Banking/Credit/Financial	Yes - Unknown #	Unknown

On October 17, 2016, we became aware of an issue regarding a systematic disbursement to alternate payee instructions that are maintained on your brokerage account. Ameriprise Financial was instructed to provide your Social Security number as an identification on this disbursement(s) to a person or entity. Due to a set up error, this identifying information was included in the address section printed on the check, which caused your Social Security number to be visible in the window of the envelope.

Attribution 1 Publication: MT AG's office Author:
Article Title: Ameriprise Financial
Article URL: <https://dojmt.gov/wp-content/uploads/Ameriprise-Financial-Services-Inc..pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-08	Backcountry Gear	OR	11/23/2016	Electronic	Business	Yes - Unknown #	Unknown

On November 4th, 2016, we were informed that customer payment card information may have been acquired without authorization. We immediately began an investigation, and confirmed that payment card information used to make online purchases on our site between September 26, 2016, and early November 5th, 2016, may have been acquired without our customer's authorization. The following information may have been accessed: payment card information, including names, payment card numbers, security codes and expiration dates. It did not include debit or credit card PINs or bank account numbers. The credit card number we have record of use for your order is a [Card Type] Card ending with [Last 4 of credit card].

Attribution 1 Publication: MT AG's office / VT AG's office Author:
Article Title: Backcountry Gear
Article URL: <https://dojmt.gov/wp-content/uploads/Back-Country-Gear.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-07	Primerica	GA	11/23/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On September 4, 2016, a Primerica agent's office was burglarized. On September 12, 2016, Primerica learned that one of the stolen devices was a computer that may have contained client files. Primerica promptly began an investigation to identify what records may have been on any stolen devices. Through the investigation, we determined that a stolen computer and external hard drive likely contained completed client and agent applications and miscellaneous files. These files contained your name and Social Security number, and may have included your driver's license or other government-issued identification number, expired debit or credit card number, medical information, checking account number, and date of birth.

Attribution 1 Publication: MT AG's office / OR AG's office Author:
Article Title: Primerica
Article URL: <https://dojmt.gov/wp-content/uploads/Primerica.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 39 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-06	Aetna Signature Administrators	CT	11/24/2016	Electronic	Medical/Healthcare	Yes - Published #	18,854

The incident occurred after an employee of Aetna Signature Administrators, a division of Aetna, mailed a CD on Sept. 6 to another employee for archiving purposes. When the envelope arrived, the CD was missing. On Sept. 9, the U.S. Postal Service was notified but was unable to locate the missing item. A "thorough investigation" revealed names, birth dates, phone numbers and some Social Security numbers were on the lost CD.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Lost CD Contained Social Security Numbers of 18,854 Health Plan Members
Article URL: <http://www.hipaajournal.com/lost-cd-contained-social-security-numbers-18854-health-plan-members-8701/>

Attribution 2 Publication: databreaches.net / chron.com / NH AG's Author:
Article Title: Aetna 'privacy incident' affects 3,000 Texans
Article URL: <http://www.chron.com/business/bizfeed/article/Aetna-data-incident-affects-3-000-Texans-10633073.php>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-05	US Navy / Hewlett Packard Enterprise Services	DC	11/23/2016	Electronic	Government/Military	Yes - Published #	134,386

Oct. 27, 2016, the Navy was notified by Hewlett Packard Enterprise Services (HPES) that one of the company's laptops operated by their employee supporting a Navy contract was reported as compromised.

Attribution 1 Publication: navy.mil Author:
Article Title: Security Breach Notification of Sailors' PII
Article URL: http://www.navy.mil/submit/display.asp?story_id=97820

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-04	Vascular Surgical Associates	GA	11/24/2016	Electronic	Medical/Healthcare	Yes - Published #	36,496

On or about September 13, 2016, we became aware of suspicious activity involving one of our computer servers. Although our investigation was not able to definitively conclude whether the hackers actually accessed or obtained a particular individual's information, it would have been possible for the hackers to access and obtain patient information about many of our current and former patients, including medical records and demographic information such as date of birth and address. No social security numbers or financial data was stored on the compromised server.

Attribution 1 Publication: databreaches.net Author:
Article Title: Vascular Surgical Associates Notifies Patients of Hack
Article URL: <https://www.databreaches.net/ga-vascular-surgical-associates-notifies-patients-of-hack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-03	Bigfork School District	MT	11/22/2016	Electronic	Educational	Yes - Unknown #	Unknown

Bigfork School District will not submit to ransom demands after the district's computer network was compromised over the weekend by ransomware. In a phone interview Tuesday, Jensen said student information affected was contained to grades and directory-type information. Staff Social Security numbers, however, were affected and as a precautionary measure personnel have been given the option to sign up for free identity protection services.

Attribution 1 Publication: dailyinterlake.com / databreaches.net Author:
Article Title: Bigfork school computers breached
Article URL: http://www.dailyinterlake.com/news/bigfork-school-computers-breached/article_d9ec72a2-b117-11e6-95cc-7be8ddd1e

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161128-02	CDCR - Folsom State Prison	CA	11/28/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

On Friday, October 28, 2016, at approximately 11 :00 a.m., the Confidential Alpha Roster (MIRS report) that contains all staff names, social security numbers, dates of birth, and other non-confidential data such as classification, tenure, and time base had been saved in a non-secure location, accessible to all FSP Staff.

Attribution 1 Publication: CA AG's office Author:
Article Title: CDCR - Folsom State Prison
Article URL: https://oag.ca.gov/system/files/BREACH%20OF%20CONFIDENTIAL%20INFORMATION_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161122-08	Madison Square Garden Company	NY	11/22/2016	Electronic	Business	Yes - Unknown #	Unknown

Findings from the investigation show external unauthorized access to MSG's payment processing system and the installation of a program that looked for payment card data as that data was being routed through the system for authorization. Data contained in the magnetic stripe on the back of payment cards swiped in person to purchase merchandise and food and beverage items at Madison Square Garden, the Theater at Madison Square Garden, Radio City Music Hall, Beacon Theater, and Chicago Theater between November 9, 2015 and October 24, 2016 may have been affected, including credit card numbers, cardholder names, expiration dates and internal verification codes.

Attribution 1 Publication: databreaches.net / CA AG's office Author:
Article Title: Madison Square Garden Company Alerts Customers of Payment Card Data Breach
Article URL: <https://www.databreaches.net/madison-square-garden-company-alerts-customers-of-payment-card-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161122-07	Conemaugh Health System / Ambucor	PA	10/31/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Ambucor Health Solutions ("Ambucor"), a remote monitoring labor service for cardiac devices utilized by Conemaugh Physician Group Cardiology, discovered that thumb drives recovered from a former employee contained some personal information of this customer's patients. The personal information may have included a patient's name, date of birth, home address, phone number, medications, race, testing data, Social Security number, patient identification number, medical device information such as the manufacturer, diagnosis, Ambucor enrollment number, Ambucor enrollment date, Ambucor technician name, physician name(s), and the name and address of the practice where the patient was seen

Attribution 1 Publication: databreaches.net / CHS website Author:
Article Title: Conemaugh Health System / Ambucor
Article URL: <http://www.conemaugh.org/press-releases/notice-of-privacy-incident>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161122-06	Stony Brook Heart Institute / University Faculty Practice	NY	11/21/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Ambucor has been investigating the activities of a former Ambucor employee, and that investigation has revealed that this former employee downloaded certain Stony Brook Internists, UFPC patient information to thumb drives and retained those drives on March 17, 2016 shortly before his employment at Ambucor ended.

Attribution 1 Publication: SBHI website / hhs.gov Author:
Article Title: Stony Brook Heart Institute / University Faculty Practice Corporation / Ambucor
Article URL: <https://heart.stonybrookmedicine.edu/patientcare/ambucor-letter>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161122-05	Northwell Health // Lenox Hill Heart and Vascular Institute /	NY	11/18/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Ambucor Health Solutions ("Ambucor"), a remote monitoring service for cardiac devices, discovered that thumb drives recovered from a former Ambucor employee contained the personal information of some of Ambucor's customer's patients. The affected patients include some patients of Stony Brook Internists, University Faculty Practice Corporation and Lenox Hill Heart and Vascular Institute.

Attribution 1 Publication: Northwell Health website Author:
Article Title: Northwell Health // Lenox Hill Heart and Vascular Institute / Ambucor
Article URL: <https://www.northwell.edu/about/news/press-releases/notice-privacy-incident>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161122-04	Main Line HealthCare / Ambucor	PA	11/11/2016	Electronic	Medical/Healthcare	Yes - Published #	4,500

Ambucor Health Solutions, a Main Line HealthCare vendor that provides remote cardiac monitoring, has been a recent victim of a patient information breach. This breach involved Ambucor patients in other parts of the United States as well as nearly 4,500 Main Line HealthCare patients who were under Ambucor's monitoring care. Ambucor has been working to investigate and take appropriate action.

Attribution 1 Publication: Main Line Health website Author:
Article Title: Ambucor Health Solutions, a Main Line HealthCare vendor, subject of patient information breach
Article URL: <https://www.mainlinehealth.org/news/2016/11/11/ambucor-health-solutions-a-main-line-healthcare-vendor-subject-of-p>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161122-03	Wentworth-Douglass Hospital / Ambucor	NH	11/21/2016	Electronic	Medical/Healthcare	Yes - Published #	775

Ambucor discovered recently that thumb drives recovered from one of its former employees contained personal information of thousands of patients nationwide, including 775 WDH patients. The personal information did not include Social Security numbers or credit card, insurance, Medicaid/Medicare or other financial information.

Attribution 1 Publication: databreaches.net Author:
Article Title: Wentworth-Douglass reports insider breach at business associate, Ambucor (UPDATED)
Article URL: <https://www.databreaches.net/wentworth-douglass-reports-insider-breach-at-business-associate-ambucor/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161122-02	Atlantis, Paradise Island (Brookfield Asset)	FL	11/21/2016	Electronic	Business	Yes - Unknown #	Unknown

The Resort began investigating unusual activity after receiving reports from its credit card processor. The Resort immediately began working with third-party forensic experts to investigate these reports and to identify any signs of compromise on its computer systems. On October 21, 2016, the Resort discovered suspicious files on its computer systems that indicated a potential compromise of customers' credit and debit card data for some credit and debit cards used at food and beverage and retail locations at the resort.

Attribution 1 Publication: VT AG's office Author:
Article Title: Atlantis, Paradise Island
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Atlantis%20Paradise%20Island%20SBN%20to%20Cons

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161122-01	Springfield Armory	IL	11/18/2016	Electronic	Business	Yes - Unknown #	Unknown

In late September, Springfield Armory received a report from a payment card network that it had noticed a pattern of unauthorized charges occurring on payment cards after they were used to make a purchase on our website. Springfield Armory immediately initiated an investigation and engaged a leading cyber security firm to examine our website network. In early October, the investigation determined that an unauthorized person gained access to the web server and installed code that was designed to copy information entered during the checkout process, including order ID, name, address, email address, phone number, payment card number, expiration date and card security code.

Attribution 1 Publication: VT AG's office / CA AG's office Author:
Article Title: Springfield Armory
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Springfield%20Armory%20SBN%20to%20Consumers.p

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161121-08	Internal Revenue Service	DC	11/20/2016	Electronic	Government/Military	Yes - Published #	8,031

A recent report from the Treasury Inspector General for Tax Administration (TIGTA) found that IRS employees sent unencrypted emails which contained 8,031 different taxpayers' personally identifiable information. According to the report, TIGTA found 326 unencrypted emails containing taxpayer data. 275 of the emails were sent internally within IRS, while 51 emails were sent outside of the agency's network to non-IRS email accounts. Of those emails sent externally, 20 were sent to six IRS employees' personal email accounts.

Attribution 1 Publication: fedsmith.com Author:
Article Title: IRS Employees Sent Unencrypted Emails Containing Personal Data of Thousands of Taxpayers
Article URL: <http://www.fedsmith.com/2016/11/20/ig-irs-employees-sent-unencrypted-emails-containing-personal-data-of-thousand>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161121-07	Briar Hill Management	MS	11/21/2016	Electronic	Medical/Healthcare	Yes - Published #	2,000

On February 26, 2016, the company learned that an employee was unable to locate a company-assigned laptop. The company later learned that the employee had violated company practice by impermissibly saving resident health information on the hard drive, and by failing to properly secure the laptop when outside of the company's office.

Attribution 1 Publication: databreaches.net / hipaajournal.com Author:
Article Title: Briar Hill Management notifies 2,000 nursing facilities residents of lost laptop
Article URL: <https://www.databreaches.net/briar-hill-management-notifies-2000-nursing-facilities-residents-of-lost-laptop/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161121-06	Biomechanics LLC / Rehab Billing Solutions	AZ	11/18/2016	Electronic	Medical/Healthcare	Yes - Published #	1,049

A Prescott physical therapy and rehabilitation firm was recently notified of a data breach by a billing and claims service vendor. The data storage account at issue contains practice information of RBS customers, including patient information from The Biomechanics LLC. Information may have included patient names, dates of birth, patient addresses, medical imaging records, intake forms, drivers' licenses, Medicare numbers, insurance cards, prescriptions, progress reports, and claim forms.

Attribution 1 Publication: dailycourier.com Author:
Article Title: Local company reports data breach in 2012 to 2014
Article URL: <http://www.dcourier.com/news/2016/nov/18/local-company-reports-data-breach-2012-2014/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161121-05	US Department of Housing and Urban Development	DC	11/18/2016	Electronic	Government/Military	Yes - Published #	600,000

The Fargo Housing and Redevelopment Authority says almost 600,000 names and social security numbers were posted to an unsecured website viewable to the public and it was not their doing but the US Department of Housing and Urban Development.

Attribution 1 Publication: Author:
Article Title: Almost 600,000 at risk of identity theft after US Department of Housing and Urban Development data breach
Article URL: <http://www.valleyhttp://www.valleynewslive.com/content/news/Almost-600000-people-at-risk-of-identity-theft-after--401>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161121-04	Gray Television	GA	8/31/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 12, 2016, Gray was notified by its insurance carrier that a package Gray had mailed to the carrier did not include a thumb drive containing employee information that was supposed to be enclosed, leading Gray to conclude that the thumb drive was either lost or stolen.

Attribution 1 Publication: SC AG's office/ MT AG's office Author:
Article Title: Gray Television
Article URL: <https://dojmt.gov/wp-content/uploads/Gray-Television.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161121-03	Odyssey Logistics & Technology Corporation	CT	4/22/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 14, 2016, W-2's (2015) for many Odyssey's employees were emailed to an unknown recipient who had impersonated Odyssey's Chief Financial Officer and his email address. As a result, this information may have been exposed to cybercriminals.

Attribution 1 Publication: SC AG's office Author:
Article Title: Odyssey Logistics & Technology Corporation
Article URL: [n/a](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161121-02	Michigan State University	MI	11/19/2016	Electronic	Educational	Yes - Published #	400,000

Michigan State University officials announced there was a massive data breach into its security system yesterday, after hackers broke through it, and gained personal information from students and employees. MSU officials say they are certain 449 people have had their personal information compromised.

Attribution 1 Publication: [fox2detroit.com / MT AG's office / CA A](#) Author:
Article Title: Michigan State University reports data breach of 400,000 records
Article URL: <http://www.fox2detroit.com/news/local-news/218427299-story>

Attribution 2 Publication: [WLNS.com](#) Author:
Article Title: MSU speaks out about security breach
Article URL: <http://wlns.com/2016/11/19/msu-speaks-out-about-security-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161121-01	Eye Institute of Marin (Marin Medical Practice Concepts)	CA	11/20/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

The San Rafael, CA-based Eye Institute of Marin has informed some of its patients that a ransomware attack on its electronic medical record provider has potentially resulted in some of their electronic protected health information being accessed by the attackers. The EMR system contained a considerable amount of sensitive patient data including names, telephone numbers, addresses, birth dates, race, gender, Social Security numbers, medical histories, medical diagnoses, prescription information, health insurance details, health visit information, charges and payment details, and emergency contact information

Attribution 1 Publication: [hipaajournal.com / CA AG's office](#) Author:
Article Title: Eye Institute of Marin Notifies Patients of Ransomware Data Loss
Article URL: <http://www.hipaajournal.com/eye-institute-marin-notifies-patients-ransomware-data-loss-3678/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-12	MYR Group	IL	5/11/2016	Electronic	Business	Yes - Published #	6,878

On May 5, 2016, we learned that on April 14, 2016, a member of the Company's payroll team received a spoofed "phishing" email message constructed to appear as if it came from the Company's CEO Bill Koertner. This employee, thinking they were responding to what appeared to be a request from the CEO for accounting, payroll and tax records, provided to the unknown third party behind the phishing email the 2015 W-2 forms for employees of the Company including your 2015 W-2 (Consumers affected per IN AG's office).

Attribution 1 Publication: [MD AG's office / IN AG's office / MT AG'](#) Author:
Article Title: MYR Group
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270416.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-11	George Gillian, DDS	AR	5/13/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

An unknown person broke into the offices of George E. Gillian, DDS and took a desktop computer containing patient dental records. In addition to dental records the stolen computer contained patient billing and payment information which included social security numbers and insurance information. As a result, your personal information may have been potentially exposed to others.

Attribution 1 Publication: [MD AG's office](#) Author:
Article Title: George Gillian, DDS
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270418.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-10	Buffalo Public School District	NY	11/18/2016	Electronic	Educational	Yes - Published #	4,400

DataBreaches.net checked the url he provided. Sure enough, there were more than 4,400 entries from the Buffalo Public Schools Language Assessment System. As indicated in the screenshot below, the records included Student ID, Student First name, Student Last Name, Parent First Name, Parent Last Name, Student Date of Birth, Student Grade, and Date of Testing.

Attribution 1 Publication: databreaches.net Author:
Article Title: Buffalo Public Schools exposed more than 4,000 records with students' and parents' personal information
Article URL: <https://www.databreaches.net/buffalo-public-schools-exposed-more-than-4000-records-with-students-and-parents-per>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-09	Lebanon Cardiology Associates, PC / Ambucor	PA	11/14/2016	Electronic	Medical/Healthcare	Yes - Published #	537

Specifically, Ambucor has been investigating the activities of a former Ambucor employee, and that investigation has revealed that in March 2016 this former employee downloaded certain Lebanon Cardiology Associates, PC patient information to mobile storage devices, often known as thumb drives or flash drives. The former employee downloaded this information shortly before his employment at Ambucor ended.

Attribution 1 Publication: hhs.gov / Ambucor Letter Author:
Article Title: Lebanon Cardiology Associates, PC
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=BA6A0FE68BB16082FC79491978505A73

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-08	Horizon Blue Cross Blue Shield of New Jersey /	NJ	11/16/2016	Paper Data	Medical/Healthcare	Yes - Published #	170,000

Between October 31 and November 2, Horizon BCBSNJ's vendor printed and mailed Explanation of Benefit letters to members; however, an error resulted in some members' names, claim numbers, Member ID numbers, dates of service, service codes, provider and facility names, and a limited description of services being printed on EOB letters that were sent to other members.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Horizon BCBS of New Jersey Privacy Breach Impacts 170,000 Members
Article URL: <http://www.hipaajournal.com/horizon-bcbs-new-jersey-privacy-breach-impacts-170000-members-3672/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-07	Emblem Health	NY	11/16/2016	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Emblem Health, one of the largest health plans in the United States, has discovered a printing error has resulted in some members Social Security numbers being printed on the outside of envelopes during a recent mailing. Affected members therefore had their Social Security numbers printed on the outside of the envelopes along with their name and address

Attribution 1 Publication: hipaajournal.com / CA AG's office Author:
Article Title: Emblem Health Mailing Error Exposes Members' Social Security Numbers
Article URL: <http://www.hipaajournal.com/emblem-health-mailing-error-exposes-members-social-security-numbers-3673/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-06	KinetoRehab Physical Therapy	NY	11/18/2016	Electronic	Medical/Healthcare	Yes - Published #	665

On September 16, 2016, KinetoRehab discovered a laptop computer was missing from its facilities. A review of security camera footage revealed the laptop computer had been stolen. The laptop contained data on a limited number of patients, although those affected by the breach have had highly sensitive information exposed. The laptop contained patients' names, birthdates, Social Security numbers, insurance information, and notes relating to the physical therapy provided by the clinic

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: Patients Notified of KinetoRehab Physical Therapy Laptop Theft
Article URL: <http://www.hipaajournal.com/patients-notified-kinetorehab-physical-therapy-laptop-theft-3677/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-05	Wal-Mart Stores, Inc.	AR	11/4/2016	Paper Data	Medical/Healthcare	Yes - Published #	771

Wal-Mart Stores, Inc AR Healthcare Provider 771 11/04/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Wal-Mart Stores, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=84334C9BAB0845D92C8AB1CAD445457C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-04	Sirius XM	NY	11/11/2016	Electronic	Business	Yes - Unknown #	Unknown

A data security incident has occurred on or about October 31, 2016 that involved a potential intrusion into your credentials in our Online Account Center (the "OAC"). Your Sirius XM customer account number, your street address, email address, nickname of your radio (i.e., your automobile radio) and your method of payment for our services (i.e., credit card or check) may have been accessed. None of your payment card or bank account data has been accessed.

Attribution 1 Publication: VT AG's office Author:
Article Title: Sirius XM
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Sirius%20XM%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-03	Chicago Public Schools	IL	11/18/2016	Electronic	Educational	Yes - Published #	30,000

An employee in the school's district shared confidential student data with the Noble Network of Charter Schools, which then used the information for a mail advertising campaign. What type of information? Students' names, addresses, grade levels and their current elementary schools.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Chicago Public School data improperly shared
Article URL: <https://www.scmagazine.com/chicago-public-school-data-improperly-shared/article/573961/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-02	QVC	PA	11/18/2016	Electronic	Business	Yes - Unknown #	Unknown

QVC uses technology to track activities that occur on its website, and the tracking technology sends data to companies that provide services to QVC. We recently learned that as the result of a technical setting, instead of sending anonymous data, the tracking technology unintentionally sent limited information about website visitors to those online marketing partners. While the information was sent securely, neither QVC nor the online marketing partners intended for this data to be sent. The information about you that was sent includes your email address and password used to access your QVC account.

Attribution 1 Publication: CA AG's office Author:
Article Title: QVC
Article URL: https://oag.ca.gov/system/files/Final%20CA%20Email%20Notice%20Proof_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161118-01	Luque Chiropractic, Inc. / Watsonville Chiropractic, Inc.	CA	11/17/2016	Electronic	Medical/Healthcare	Yes - Published #	1,341

On September 18, 2016, Luque was notified by its billing software company that its Amazon "S3" storage account was vulnerable because it was accessible to persons outside their organization, and that a security researcher accessed and downloaded information from the storage account. This storage account contained, among other things, protected health information of certain Luque Chiropractic, Inc. and Watsonville Chiropractic, Inc. (David W. Christie, D.C.) patients. While Luque has no indications that any fraud has resulted from this incident, it has confirmed that the data affected by this incident possibly includes patient names, addresses, diagnoses, dates of birth, treatment locations, treatment dates, and Social Security numbers.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
Article Title: Luque Chiropractic, Inc. / Watsonville Chiropractic, Inc.
Article URL: https://oag.ca.gov/system/files/Luque%20--%20Press%20Release_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-11	Indiana Health Coverage Program / HP Enterprise	TX	11/7/2016	Electronic	Medical/Healthcare	Yes - Published #	1,235

HP Enterprise Services LLC (HPE), a Medicaid fiscal agent for the Indiana Health Coverage Program, recently notified HHS of the theft of 1,235 members' information. The theft was discovered on September 16 and reported to HHS by HPE on November 7.

Attribution 1 Publication: hhs.gov / IN AG's office / databreaches. Author:
Article Title: HP Enterprise Services, LLC
Article URL: <https://www.databreaches.net/indiana-health-coverage-program-members-notified-of-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-10	HeartCare Consultants	FL	5/11/2016	Electronic	Medical/Healthcare	Yes - Published #	16,000

HeartCare Consultants FL Healthcare Provider 16000 05/11/2016 Hacking/IT Incident Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: HeartCare Consultants
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-09	Harrisonburg OB GYN Associates, P.C.	VA	10/20/2016	Electronic	Medical/Healthcare	Yes - Published #	800

Harrisonburg OB GYN Associates, P.C. VA Healthcare Provider 800 10/20/2016 Theft Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: Harrisonburg OB GYN Associates, P.C.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-08	Kaiser Permanente Health Plan, Inc. (Northern)	CA	11/7/2016	Electronic	Medical/Healthcare	Yes - Published #	4,432

Kaiser Permanente is notifying some of its members of a website configuration error that resulted in the exposure of some of their protected health information. Fortunately, the error was rapidly identified and ePHI was only exposed for around two hours. The extent of ePHI exposed depends on the webpages members visited after logging in, although the exposed information was limited in nature and did not include any highly sensitive data such as Social Security numbers or financial information.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Kaiser Permanente Health Plan, Inc. of Northern California
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf?jsessionid=2BF328FC76110BB77CC9918BFCE06C2A

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-07	Kaiser Permanente Health Plan, Inc. (Southern)	CA	11/6/2016	Electronic	Medical/Healthcare	Yes - Published #	3,044

Kaiser Permanente is notifying some of its members of a website configuration error that resulted in the exposure of some of their protected health information. Fortunately, the error was rapidly identified and ePHI was only exposed for around two hours. The extent of ePHI exposed depends on the webpages members visited after logging in, although the exposed information was limited in nature and did not include any highly sensitive data such as Social Security numbers or financial information.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Kaiser Permanente Health Plan, Inc. (Southern California)
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf?jsessionid=2BF328FC76110BB77CC9918BFCE06C2A

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-06	Austin Pulmonary Consultants	TX	11/7/2016	Paper Data	Medical/Healthcare	Yes - Published #	889

On September 8, 2016 Austin Pulmonary Consultants discovered that a third party vendor which had been contracted to provide cleaning services at its recently opened offices at 5920 W. William Cannon, Building 1, Suite 150 in Austin, Texas had improperly disposed of documents containing the protected health information of patients.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Austin Pulmonary Consultants Reports Improper Disposal of PHI
Article URL: <http://www.hipaajournal.com/austin-pulmonary-consultants-improper-disposal-phi-3670/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 47 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-05	Best Health Physical Therapy, LLC / Rehab Billing	CT	11/10/2016	Electronic	Medical/Healthcare	Yes - Published #	1,100

The data breach occurred at Best Health Physical Therapy's billing service provider, Rehab Billing Solutions (RBS). Best Health Physical Therapy was notified of the breach on September 23, 2016 after RBS was contacted by MacKeeper security researcher Chris Vickery and advised that client data had been exposed and was freely accessible online.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](http://hhs.gov/hipaajournal.com) Author:
Article Title: Best Health Physical Therapy Fires Billing Service Provider for PHI Breach
Article URL: <http://www.hipaajournal.com/best-health-physical-therapy-fires-billing-service-provider-for-phi-breach-3671/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-04	Windy Ridge Accounting & Tax Service	OR	11/9/2016	Electronic	Business	Yes - Unknown #	Unknown

Someone broke into our office between 1am on October 22nd and 1 am on October 23rd 2016, and stole all our computers and other electronics and a small number of actual files (any clients whose files were stolen have been notified their actual file is gone). The information included your name, Social Security number, address, date of birth, and banking account information for clients who use direct deposit.

Attribution 1 Publication: OR AG's office Author:
Article Title: Windy Ridge Accounting & Tax Service
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/2117860618>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-03	Honig's Whistle Stop, Inc.	MI	11/8/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 5, 2016, we confirmed through our forensic investigators that our website had been breached. The incident involved an outside source uploading a malicious file on Honig's Whistle Stop, Inc.'s ("Honig's") website that collected information entered on our customer order form.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Honig's Whistle Stop, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Honigs%20Whistle%20Stop%20SBN%20to%20Consum

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-02	Baxter Credit Union	CA	10/3/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On October 11, 2016, we learned that the email account of one of our employees had been compromised as part of an investigation we undertook after the email account was used to SPAM, or send an unsolicited email. The account contained certain personal information including names, or partial names, Social Security numbers and, for some individuals, a bank account number, credit card number and/or driver's license number.

Attribution 1 Publication: CA AG's office Author:
Article Title: Baxter Credit Union
Article URL: <https://oag.ca.gov/system/files/BCU - SSN Plus Notice 0.PDF?>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161115-01	Eileen Fisher	NY	10/24/2016	Electronic	Business	Yes - Unknown #	Unknown

Our records show that you made a purchase on eileenfisher.com between Wednesday, September 7 – Monday, October 24, 2016. In late October, we were informed of a possible data security incident that affected our website during that time.

Attribution 1 Publication: CA AG's office / VT AG's office Author:
Article Title: Eileen Fisher
Article URL: https://oag.ca.gov/system/files/Eileen%20Fisher%20notice%20only_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 48 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161114-02	Broward Health Imperial Point	FL	11/10/2016	Paper Data	Medical/Healthcare	Yes - Published #	126

Earlier this year, law enforcement officers visited the home of an individual as part of a routine investigation and discovered documents containing the personal information of patients of Broward Health Imperial Point in Fort Lauderdale, Florida. According to the Florida Bulldog, the documents were hospital facesheets which contained patients' names, addresses, phone numbers, dates of birth, Social Security numbers, insurers' names, insurance guarantor details, emergency contact information, and reasons for visits.

Attribution 1 Publication: hipaajournal.com / Scmagazine.com Author:
Article Title: Broward Health Discovers Breach 'Linked' to Florida Identity Theft Gang
Article URL: <http://www.hipaajournal.com/broward-health-discovers-breach-linked-to-florida-identity-theft-gang-3665/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161114-01	Seguin Dermatology	TX	11/14/2016	Electronic	Medical/Healthcare	Yes - Published #	29,969

Texas-based Seguin Dermatology has started informing patients of a ransomware attack that has likely resulted in electronic protected health information (ePHI) being inappropriately accessed. The attack occurred on or around September 12, 2016 and involved a server used by the office of Robert J. Magnon, M.D. The ransomware encrypted numerous file types preventing data access. While the server was not used to store electronic medical records, some ePHI was in the encrypted files.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Ransomware Attack: ePHI Access Likely
Article URL: <http://www.hipaajournal.com/sequin-dermatology-announces-ransomware-attack-ephi-access-likely-3669/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161109-02	VA Eastern Colorado Health Care System	CO	11/9/2016	Electronic	Government/Military	Yes - Published #	2,130

More than 2,100 Colorado veterans may have had their personal information compromised, the VA Eastern Colorado Health Care System (ECHCS) said Wednesday. At risk are the veterans' names, the last four digits of their Social Security number and their diagnoses. According to the ECHCS, the information may have been compromised when a VA employee emailed unencrypted documents to their personal email account

Attribution 1 Publication: databreaches.net / KKTv.com Author:
Article Title: Personal information for thousands of Colorado vets may have been compromised
Article URL: <http://www.kktv.com/content/news/Personal-information-for-thousands-of-Colorado-vets-may-have-been-compromise>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161109-01	UFCW Local 655	MO	7/14/2016	Electronic	Business	Yes - Unknown #	Unknown

On or around July 21, 2016, UFCW Local 655 Food Employers Joint Pension Plan was the victim of a ransomware attack. After an extensive investigation, we found no evidence demonstrating that an unauthorized individual accessed or acquired your child's information, however we determined that an unauthorized user gained access to our server on July 14, 2016, one week before the ransomware attack. While there is no evidence that your child's information was accessed or acquired, we are unable to definitively rule out this possibility, and are providing notice out of an abundance of caution.

Attribution 1 Publication: CA AG's office / VT AG's office / OR AG' Author:
Article Title: UFCW Local 655
Article URL: https://oag.ca.gov/system/files/UFCW%20Local%20655%20Food%20Employers%20notice%20only%20pdf_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161108-04	Prime Inc.	MO	10/31/2016	Electronic	Business	Yes - Unknown #	Unknown

On the morning of October 20, 2016 Prime encountered a cyber-attack. At this time, an unauthorized, external user breached the Prime network and was successful in accessing data/information respecting the driver identities of Prime company drivers who were on active status with the company during calendar year 2015.

Attribution 1 Publication: Nh AG's office Author:
Article Title: Prime Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/prime-20161031.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161108-03	Morris Rothenberg & Son, Inc. dba Rothco	NY	11/3/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 26, 2016, Rothco learned of an intrusion to its website that may have resulted in the disclosure of users' credit card numbers. The incident involved individuals' names, addresses and credit card numbers. The incident did not involve Social Security numbers.

Attribution 1 Publication: NH AG's office Author:
Article Title: Morris Rothenberg & Son, Inc. dba Rothco
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/morris-rothenberg-son-20161103.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161108-02	DealerBuilt / Auto Dealerships Nationwide	IA	11/8/2016	Electronic	Business	Yes - Unknown #	Unknown

Names, addresses, phone numbers and social security numbers for both customers and employees for over a hundred car dealerships have leaked online, all thanks to a centralized records system coupled with shoddy security. Each database includes dozens of tables each, including sales, messages between staff (including talk of bonuses in some cases), payroll data, and customer names and addresses. The databases also stored sensitive information like social security numbers of customers, but also the employees who work at these dealerships.

Attribution 1 Publication: databreaches.net / Zdnet.com Author:
Article Title: Bought a car recently? Millions of dealership customer details found online
Article URL: <http://www.zdnet.com/article/bought-a-car-recently-millions-of-customers-records-found-online/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161108-01	Kaiser Foundation Health Plan of the Northwest	OR	10/12/2016	Electronic	Medical/Healthcare	Yes - Published #	544

For approximately two hours during the evening of October 12th into the early morning of October 13th, 2016, some of your protected health information that you viewed after signing in to kp.org may have been mistakenly viewable by other visitors to the website during that time frame.

Attribution 1 Publication: CA AG's office / OR AG's office / hipaajo Author:
Article Title: Kaiser Foundation Health Plan of the Northwest
Article URL: https://oag.ca.gov/system/files/Privacy_Incident_Oct_2016_Template_Member_Letter_Standard_Custom_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161107-09	Sentinel Hotel	OR	11/4/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 5, 2016, the investigation identified signs that an unauthorized program was installed on one of the payment terminals at the hotel's front-desk designed to copy data as it was input into the terminal. The program could have copied payment card data – including cardholder name, payment card account number, card expiration date, and verification code – of guests who used a payment card at this one terminal during the period from July 12, 2016 to October 3, 2016.

Attribution 1 Publication: databreaches.net / OR AG's office Author:
Article Title: Sentinel Hotel Notifies Guests of Payment Card Incident
Article URL: <https://www.databreaches.net/or-sentinel-hotel-notifies-guests-of-payment-card-incident/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161107-08	Thirty Three Threads, Inc.	CA	11/2/2016	Electronic	Business	Yes - Unknown #	Unknown

Between approximately September 22, 2016, and October 5, 2016, we believe our internet system was hacked into, and that a breach occurred that may have exposed some of your personal information. The IT company was able to remove the planted code that had caused the issue and have stopped the breach. The data accessed included your: (i) date of online purchase; (ii) billing name; (iii) shipping name; (iv) shipping address; (v) purchase amount; (vi) email address; and (vii) credit card number and security code. In some instances, an account ID number was also accessed.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Thirty Three Threads, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Thirty%20Three%20Threads.%20Inc.%20SBN%20to%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161107-07	Manduka	CA	10/31/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 28, 2016, Manduka learned of a potential security incident involving the unauthorized installation of malware on our e-commerce web platform. While our investigation is ongoing, we believe the malware could have compromised personal information of some of our customers who utilized our web platform to purchase products from January 29, 2016- October 8, 2016, including first and last name, address, website login credentials (username and password), credit/debit card number, expiration date, and CVV security code.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Manduka
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Manduka%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161107-06	i-Dressup.com	US	11/6/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 27, 2016, we learned that cyber criminals gained unauthorized access to our computer system and to your personal information, including your age, email address and password that you provided to create, and used to access, your www.i-dressup.com account, as well as any additional personal information that you may have voluntarily provided such as your first name, last name, gender and country (collectively, "Personal Information").

Attribution 1 Publication: CA AG's office Author:
Article Title: i-Dressup.com
Article URL: https://oag.ca.gov/system/files/Notice%20of%20i-dressup_data_breach_C_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161107-05	Welk Resort Group	CA	10/5/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 6, 2016, we learned that, late on October 5, a Welk team member's home was burglarized, and the team member's company laptop was stolen. The information contained on the stolen laptop may include your name, Social Security number, address, certain benefit plan participation information, and date of birth.

Attribution 1 Publication: CA AG's office Author:
Article Title: Welk Resort Group
Article URL: https://oag.ca.gov/system/files/Welk%20CA%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161107-04	National Wholesale Incorporated	NC	10/15/2016	Electronic	Business	Yes - Published #	14,281

Findings from the investigation show that if a customer placed an order on our website from September 1, 2016 through October 15, 2016, information associated with the order being placed, including the customer's name, address, phone number, email address, payment card number, expiration date and credit card security code (CVV) may have been obtained by unauthorized individuals.

Attribution 1 Publication: CA AG's office / VT AG's office / NH AG' Author:
Article Title: National Wholesale Incorporated
Article URL: https://oag.ca.gov/system/files/CA%20Consumer%20Notice_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161107-03	Singh and Arora Oncology Hematology, PC	MI	10/21/2016	Electronic	Medical/Healthcare	Yes - Published #	16,000

Singh and Arora Oncology Hematology, P.C. MI Healthcare Provider 16000 10/21/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
 Article Title: Singh and Arora Oncology Hematology, PC
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161107-02	MGA Home Healthcare	AZ	10/19/2016	Electronic	Medical/Healthcare	Yes - Published #	3,119

MGA Home Healthcare has notified 3,119 patients that some of their electronic protected health information (ePHI) has been exposed after an unencrypted laptop computer was stolen from the vehicle of an employee.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
 Article Title: Theft of Unencrypted Laptop Results in Exposure of 3,100 Patients' ePHI
 Article URL: <http://www.hipaajournal.com/theft-of-unencrypted-laptop-results-in-exposure-of-3100-patients-ephi/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161107-01	Four Star Drug of Bethany, Inc.	NE	10/18/2016	Paper Data	Medical/Healthcare	Yes - Published #	647

Four Star Drug of Bethany, Inc. NE Healthcare Provider 647 10/18/2016 Improper Disposal Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: Four Star Drug of Bethany, Inc.
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161101-05	You and Your Health Family Care, Inc.	FL	10/20/2016	Electronic	Medical/Healthcare	Yes - Published #	3,000

You and Your Health Family Care, Inc. FL Healthcare Provider 3000 10/20/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
 Article Title: You and Your Health Family Care, Inc.
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161101-04	Office of Dr. Dennis T. Myers, DDS, PA	MO	10/24/2016	Electronic	Medical/Healthcare	Yes - Published #	3,364

Dr. Dennis T. Myers, D.D.S., P.A. MO Healthcare Provider 3364 10/24/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
 Article Title: Office of Dr. Dennis T. Myers, DDS, PA
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161101-03	Anthem	IN	10/26/2016	Electronic	Medical/Healthcare	Yes - Published #	3,525

Anthem, Inc. IN Health Plan 3525 10/26/2016 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: Anthem
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161101-02	Don Joses Mexican Restaurant	TX	11/1/2016	Paper Data	Business	Yes - Unknown #	Unknown

It was a startling surprise for neighbors who found papers containing social security numbers, bank accounts, and other personal information blowing across their yards over the weekend. "There were signed receipts, credit card, MasterCard, Visa, invoices, W2's, income tax stuff," Roberts said.
Along with social security numbers, routing numbers and checks from the restaurant.

Attribution 1 Publication: databreaches.net / newschanneltnow.co Author:
Article Title: Popular restaurant under fire after dumpster discovery
Article URL: <http://www.newschannel6now.com/story/33534559/popular-restaurant-under-fire-after-dumpster-discovery>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161101-01	City of Duluth	MN	11/1/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

The breach occurred on Aug. 14 and was discovered eight days later, at which time the compromised email account was shut down immediately. An ensuing investigation determined that the email intruder could have accessed several potentially sensitive documents, including: A voter registration list that contained 55,184 voter names, addresses, phone numbers and dates of birth; A business license report that contained about 427 business names, addresses, some Social Security numbers and tax ID numbers; Four business license applications that contained names, addresses, birth dates, tax ID numbers, Social Security numbers and driver's license or passport numbers; Job applicant information for 14 people, containing personal contact information, driver's license numbers and questionnaire responses. Included in some of the documents were 184 Social Security numbers.

Attribution 1 Publication: bemidjipioneer.com Author:
Article Title: Duluth phishing attack may have exposed private data: City acknowledges security breach in letter to voters
Article URL: <http://www.bemidjipioneer.com/news/region/4149410-duluth-phishing-attack-may-have-exposed-private-data-city-ackn>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-16	Stream Gas & Electric	TX	5/13/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 25, 2016, we discovered that an unauthorized person gained access to the employee website hosted by our payroll and benefits provider, ExponentHR. Based on our ongoing investigation, we determined that during the period from April 21, 2016 to April 25, 2016 the unauthorized person may have accessed current and former employees' account information on the ExponentHR website, and for a small percentage of accounts, attempted to change the direct deposit information. The information involved in this incident includes the information in your ExponentHR account, including your name, address, date of birth, Social Security number, bank account and routing number, date of birth, and wages.

Attribution 1 Publication: MD AG's office Author:
Article Title: Stream Gas & Electric
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270419.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-15	Kolodzey & Cox CPAs, PC	NJ	5/17/2016	Electronic	Business	Yes - Unknown #	Unknown

On May 2, 2016, with the help of third party computer forensic experts, K & C learned that a possible security incident may have impacted the security of client information stored on its servers. It appears that a limited number of files stored on K & C's system may have been accessed by an unauthorized individual on March 21, 2016. These files contain information related to tax filings, and may have included clients' name, address, Social Security number, wage information, and in some instances bank account information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Kolodzey & Cox CPAs, PC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270423.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 53 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-14	Batdorf & Bronson Coffee Roasters	WA	5/17/2016	Electronic	Business	Yes - Published #	1,845

On April 20, 2016, we learned that an unknown attacker had compromised our e-commerce system, potentially affecting customer payment card information. The information compromised by the attack may have included your name, payment card number, expiration date, and CVV number from payment cards used for online transactions on Batdorf's e-commerce web site from October 1, 2015 to April 22, 2016 (Consumers affected per IN AG's office)

Attribution 1 Publication: MD AG's office / IN AG's office Author:
Article Title: Batdorf & Bronson Coffee Roasters
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270424.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-13	USI Insurance Services / Unvers Workplace Solutions	NY	5/19/2016	Electronic	Business	Yes - Published #	1,851

On April 28, 2016, the payroll representative mistakenly emailed to the Employee an attachment containing the W2 Forms of other USI Insurance Services employees. You are receiving this notice because your W2 Form was included in the attachment. As you know, your W2 Form includes, among other information, your name, Social Security number and employee tax information. (Consumers affected per IN AG's office)

Attribution 1 Publication: MD AG's office / IN AG's office Author:
Article Title: USI Insurance Services
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270425.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-12	Oldcastle Building Envelope	GA	5/18/2016	Electronic	Business	Yes - Unknown #	Unknown

We have just learned that last Thursday, through a sophisticated attack directed at our payroll department, a database containing your 2015 W2 information, including your Social Security number, may have been accessed by criminals engaged in tax or related fraud. We have not seen any cases yet of misuse of the information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Oldcastle Building Envelope
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270427\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270427(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-11	Mid-Ohio Foodbank	OH	5/24/2016	Electronic	Business	Yes - Unknown #	Unknown

Our client, Mid-Ohio Foodbank, on April 12, 2016, learned that an employee's password protected, company issued laptop, stolen on March 14, 2016, contained applicant benefit files. The employee reported that a suitcase with the laptop was checked on a flight, and upon reaching the employee's destination, learned that the laptop was stolen from the suitcase. To date, the laptop has not been recovered. The information contained in the benefit files included applicants' names, addresses, driver's license, or Social Security numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Mid-Ohio Foodbank
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270428.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-10	Ben Bridge Jewelers	WA	5/27/2016	Electronic	Business	Yes - Unknown #	Unknown

On Wednesday, May 18, 2016, Ben Bridge was the target of an e-mail phishing attack that resulted in the disclosure of certain of its current and former employees' 2015 W-2 forms, including those employees' first and last names, addresses, Social Security numbers and compensation information. Upon discovering the incident, Ben Bridge promptly launched an internal investigation and notified the Federal Bureau of Investigation ("FBI") and the Internal Revenue Service ("IRS")

Attribution 1 Publication: MD AG's office Author:
Article Title: Ben Bridge Jewelers
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270431.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-09	Symphony Health Solutions Corporation	PA	5/4/2016	Electronic	Medical/Healthcare	Yes - Published #	365

On April 22, 2016, an employee of Symphony Health Solutions Corporation ("SHS") received a targeted fraudulent email requesting copies of W-2 forms for certain current and former personnel of SHS. The employee responded with PDF attachments of W-2s of approximately 365 individuals, of which 2 are residents of Maryland. The following personal information was involved in the incident: names, addresses, wages, and social security numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Symphony Health Solutions Corporation
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270439.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-08	AxoGen	FL	4/19/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On April 5, 2016 AxoGen discovered that on March 17, 2016, as a result of a phishing email, an unauthorized third party obtained an electronic file containing certain information on individuals that were employed by AxoGen during 2015. AxoGen has confirmed that the information obtained by the unauthorized party included 2015 W-2, which included full names, Social Security numbers, home addresses, and wage and tax information.

Attribution 1 Publication: MD AG's office Author:
Article Title: AxoGen
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270441.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-07	Anthelio Healthcare Solutions, Inc.	TX	4/20/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On April 4, 2016 Anthelio discovered that on February 25, 2016, as a result of a phishing incident, an unauthorized third party may have received an electronic file containing certain information on current and former employees who received employment earnings in 2015 from Anthelio.

Attribution 1 Publication: MD AG's office Author:
Article Title: Anthelio Healthcare Solutions, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270448.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-06	Abernathy & Company	AR	5/11/2016	Electronic	Business	Yes - Unknown #	Unknown

bernathy recently noticed some unusual activity on its computer system. Upon learning of the issue, Abernathy immediately commenced an investigation of the incident, including engaging external cybersecurity professionals, and retained an independent computer forensic firm to determine if any information was at risk. On April 12, 2016 Abernathy received notification that the forensic investigation concluded that an unauthorized third-party had accessed the server and obtained certain client information in a file.

Attribution 1 Publication: MD AG's office Author:
Article Title: Abernathy & Company
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270457.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-05	Office of the Comptroller of the Currency	DC	10/28/2016	Electronic	Government/Military	Yes - Published #	10,000

The top U.S. banking regulator revealed Friday that a former employee downloaded thousands of files from the agency's servers without authorization nearly a year ago and that the agency has not yet been able to recover those files.

Attribution 1 Publication: housingwire.com Author:
Article Title: OCC reveals major information security breach involving former employee
Article URL: <http://www.housingwire.com/articles/38402-occ-reveals-major-information-security-breach-involving-former-employee>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-04	New Leaders	NY	4/15/2016	Electronic	Business	Yes - Unknown #	Unknown

We have learned that a cybercriminal using a spoofing scam led to an unauthorized third party obtaining certain W-2 information from 2014 and 2015 for New Leaders current and former employees.

Attribution 1 Publication: MD AG's office Author:
Article Title: New Leaders
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270443.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-03	Politi & Magnifico LLC	CT	10/28/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 13, 2016, we discovered that a small number of our clients' 2015 tax returns were filed with the IRS by an unknown third party. Your 2015 tax return was not among those returns filed. Upon learning of the unauthorized tax filings we took immediate steps to investigate the cause and scope of the issue and contacted law enforcement. Our investigation has determined that information contained in your tax documents may have been exposed including your name, address, date of birth, Social Security number and limited financial information.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Politi & Magnifico LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Politi%20%20Magnifico%20SBN%20to%20Consumer

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-02	Office of Anne M. Cummings, MD, FACP / Marin Medical	CA	10/30/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On August 22, 2016, I received confirmed notice from my electronic medical record provider that their electronic system was subject to a malware attack on July 26, 2016. They became aware of the incident on July 27, 2016, and I am informed that they promptly took action to secure their systems. The electronic record system contains your full name, address, telephone number, date of birth, gender, race, social security number (if provided to us), medical history, prescriptions, diagnoses, insurance and health visit information, emergency contact information, and charges and payments. The system does not contain personal financial information (i.e. no credit card nor bank information).

Attribution 1 Publication: CA AG's office Author:
Article Title: Office of Anne M. Cummings, MD, FACP
Article URL: https://oag.ca.gov/system/files/Cummings%20Notice%20A_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161031-01	Beyond Yoga	CA	10/28/2016	Electronic	Business	Yes - Unknown #	Unknown

What Happened? We recently discovered that your personal information may have been exposed in July and August 2016 as a result of an incident currently under investigation. What Information Was Involved? The incident may have exposed your personal information, including payment card information and user names and passwords.

Attribution 1 Publication: CA AG's office Author:
Article Title: Beyond Yoga
Article URL: https://oag.ca.gov/system/files/password-reset-email_V3_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 56 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161028-4	Spectrum, Inc.	CA	5/23/2016	Electronic	Business	Yes - Unknown #	Unknown

Between April 4, 2016 and April 21, 2016, the company was subject to a phishing scam in which hackers, impersonating company executives, were able to obtain copies of W-2 tax forms of all of our company employees. We became aware of this data breach on April 26, 2016. We believe that the hackers may attempt to file fraudulent tax returns with the IRS or with state taxing authorities in the name of some of the employees in order to obtain a tax refund (which refund would be sent to the hackers).

Attribution 1 Publication: MD AG's office Author:
Article Title: Spectrum, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270463.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161028-06	Habitat for Humanity	MI	10/28/2016	Electronic	Business	Yes - Published #	5,500

Habitat for Humanity of Michigan's virtual hard drive backups, which contained more than 400GB of information, were discovered online by an Austin-based security researcher in early October. The data is said to have contained hundreds of background and credit check profiles, in addition to roughly 4,600 individual profiles, all of which included Social Security numbers and other personally identifiable information.

Attribution 1 Publication: dailydot.com Author:
Article Title: More than 5,000 people exposed in Habitat for Humanity data breach
Article URL: <http://www.dailydot.com/layer8/habitat-for-humanity-applicants-michigan-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161028-05	Hill+Knowlton	NY	4/29/2016	Electronic	Business	Yes - Published #	592

Please be advised that on February 23, 2016, an employee of Hill+Knowlton Strategies sent certain employee records to an unauthorized email recipient. The incident was not discovered until Friday, April 22, 2016. The documents contained certain personal information of Hill+Knowlton Strategies employees including names, home addresses, social security numbers and salary information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Hill+Knowlton
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270458.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161028-03	Napoli Bern Ripka Shkolnik, LLP	NY	6/6/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 9, 2014, Pasternack Tilker, LLP discovered that a now former employee of the law firm Napoli Bern Ripka Shkolnik, LLP ("Napoli Bern"), removed certain client data from a network system shared between our firm and Napoli Bern without authorization from either law firm.

Attribution 1 Publication: MD AG's office Author:
Article Title: Napoli Bern Ripka Shkolnik, LLP
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270474.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161028-02	37th Parallel Properties Investment Group, LLC	VA	6/7/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On May 9, 2016, we discovered that an unauthorized third party had accessed an email account belonging to one of our employees. Our investigation suggests the unauthorized party first gained access on or before April 25, 2016. The data accessed may have included personal information such as your first and last name, email address, account number(s) and social security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: 37th Parallel Properties Investment Group, LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270477.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161028-01	Marymount University	VA	6/3/2016	Electronic	Educational	Yes - Unknown #	Unknown

We recently learned that an unauthorized individual may have gained access to some of our systems during two brief overnight periods on May 13 to May 14, 2016 and May 15 to May 16, 2016. We believe that the incident may have affected certain employees' personal information available on our intranet, including name, address, phone number, email address, Social Security number, wage information, and, for some employees, bank account information and the name and Social Security number of their spouse and dependents.

Attribution 1 Publication: MD AG's office Author:
Article Title: Marymount University
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270471%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270471%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161027-02	Rocky Mountain Credit Union	MT	10/26/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

A southwestern Montana credit union has notified 135 of its members that some of their personal information could have been publicly accessible through its website between April 15 and June 30.

Attribution 1 Publication: washingtontimes.com / MT AG's office Author:
Article Title: Rocky Mountain Credit Union
Article URL: <http://www.washingtontimes.com/news/2016/oct/26/credit-union-tells-customers-about-possible-securi/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161027-01	Finley Center for Acupuncture and	NV	10/20/2016	Electronic	Medical/Healthcare	Yes - Published #	3,000

Earlier this month, The Finley Center in Nevada, a provider of physical therapy, acupuncture, and naturopathic medicine, reported the theft of a desktop computer to the Office for Civil Rights. The computer contained the ePHI of approximately 3,000 patients

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Recent Healthcare Data Breaches Involving the Theft of Unencrypted Devices used to Store ePHI
Article URL: <http://www.hipaajournal.com/theft-of-unencrypted-laptop-results-in-exposure-of-3100-patients-ephi/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161026-07	SOS International LLC	NY	10/20/2016	Electronic	Business	Yes - Unknown #	Unknown

Beginning in mid-August 2016, SOSi began using the Egnyte™ file-sharing platform to facilitate renewing and extending these contracts. In September 2016, SOSi experienced a data incident involving the Egnyte™ file-sharing platform, in which personal information contained in contract materials uploaded to an EgnyteM folder by some SOSi independent contractors may have been accessed or downloaded from Egnyte™ by other SOSi independent contractors.

Attribution 1 Publication: NH AG's office Author:
Article Title: SOS International LLC
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/sos-international-20161020.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161026-06	ParsonsKellogg	RI	10/18/2016	Electronic	Business	Yes - Unknown #	Unknown

I write to provide notice of a data security incident in accord on behalf of my client parsonsKellogg, llc. One service parsonsKellogg provides is establishing webstores or microsities for companies which allow their employees to order promotional products bearing the employer's logo. For many customers, employees use their own credit card to pay for the order.

Attribution 1 Publication: NH AG's office Author:
Article Title: ParsonsKellogg
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/parsonskellogg-20161018.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161026-05	Greater Florida Anesthesiologists	FL	10/21/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On September 21, 2016, GFA learned that a third party may have gained unauthorized access to files contained on the GFA computer systems on July 12, 2016. GFA immediately began an investigation, including hiring a leading forensics firm, which determined that the files may have contained GFA employees' names, dates of birth, social security numbers, bank account information, and potentially benefits and other financial information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Greater Florida Anesthesiologists
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/greater-fl-anesthesiologists-20161021.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161026-04	Atlanta Falcons Football Club, LLC / NCR Corporation	GA	10/21/2016	Electronic	Business	Yes - Published #	975

On September 30, 2016, we were notified by our service provider that operated the online store system, NCR Corporation, that an unauthorized third party uploaded malicious computer code to the system that hosts officialfalcons.com. The code was present when customers made purchases on the website and may have been used to obtain customer information.

Attribution 1 Publication: NH AG's office / MT AG's office Author:
Article Title: Atlanta Falcons Football Club, LLC
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/atlanta-falcons-20161021.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161026-03	Bedford County Board of Education	TN	10/12/2016	Paper Data	Educational	Yes - Published #	862

Bedford County Board of Education TN Business Associate 862 10/12/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Bedford County Board of Education
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161026-02	Medical Marijuana Dispensary	AZ	10/25/2016	Paper Data	Business	Yes - Unknown #	Unknown

A medical marijuana dispensary is conducting an investigation into how sensitive patient information ended up in a pile of trash on a public sidewalk. The man who found the medical records believes this is a breach of patient privacy. The documents weren't shredded and were laying out in the open. Somehow, trash from Horizon THC, a medical marijuana dispensary near 31st Avenue and Peoria, ended up in a pile of garbage across the street and visible from the sidewalk.

Attribution 1 Publication: Fox10phoenix.com Author:
Article Title: Medical marijuana patients' personal information found in trash pile
Article URL: <http://www.fox10phoenix.com/news/arizona-news/213622501-story>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161026-01	Cisco Systems	CA	8/18/2016	Electronic	Business	Yes - Unknown #	Unknown

An independent security researcher discovered that a limited set of job application related information from the Cisco Professional Careers mobile website was accessible. Exposed data included the following data fields: name, address, email, phone number, username and password, answers to security questions, education and professional profile, cover letter and resume text, and voluntary information (if entered) such as gender, race, veteran status, and disability.

Attribution 1 Publication: CA AG's office / databreaches.net Author:
Article Title: Cisco Systems
Article URL: https://oag.ca.gov/system/files/%28US%29%20Data%20Incident%20-%20Notice%20to%20Consumers_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 59 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161025-03	City of Middletown	NY	10/21/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

On Wednesday, June 15, 2016, the City of Middletown was notified by the FBI that it had discovered evidence that the City of Middletown network may have been compromised. The investigation revealed that an unauthorized individual or individuals gained access to a database in Middletown's system that contained some of your personal information and was able to export at least a portion of the information in the database. The following types of your information accessible to the unauthorized individual(s) included: <<ClientDef1(your name, Social Security number, drivers license number, state ID number, date of birth, FBI number and address.)>>

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: City of Middletown
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Middletown%20New%20York%20SBN%20to%20Consu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161025-02	TOPCON / Paychex	CA	10/19/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 26, 2016, we learned of unauthorized changes to the direct deposit information of some employee accounts in the Paychex payroll system. We immediately launched an investigation to determine the nature and scope of this incident. While our investigation is ongoing, we determined that, on August 12, 2016, certain accounts were accessed without authorization using compromised administrative credentials.

Attribution 1 Publication: VT AG's office Author:
Article Title: TOPCON
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Topcon%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161025-01	Silver Creek Physical Therapy Entities	CA	9/11/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On September 11, 2016, we were notified by our billing and software companies that their Amazon "S3" storage account was vulnerable because it was accessible to persons outside their organization, and that a security researcher who works for a software company accessed and downloaded information from the account. This storage account contained, among other things, protected health information of certain Silver Creek Fitness & Physical Therapy, Silver Creek Physical Therapy Gilroy, Silver Creek Physical Therapy Sunnyvale, and Silver Creek Physical Therapy Los Gatos patients.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Silver Creek
Article URL: https://oag.ca.gov/system/files/Adult%20Notice_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-16	Zero Gravity Solutions	FL	7/29/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 1, 2016, a person falsely claiming to offer information technology support to one of Zero Gravity's employees obtained administrative access via remote login to the employee's laptop computer and its hard drive, which contained data including personal information of investors in the company. While the types of personal information contained on the affected laptop varied from investor to investor, the information on the computer's hard drive included name, address, phone number, email address, citizenship, and social security number or other government-issued identification number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Zero Gravity Solutions
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271146.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-15	New America	CA	7/19/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 3, 2016, New America discovered that an unknown party had accessed a limited number of its employee email accounts without authorization. This access occurred on or about January 18. On June 8, 2016, our subsequent investigation concluded that the accounts contained your Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: New America
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271751%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271751%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-14	Clear One Funding, LP / WWC Capital Group, LLC	VA	7/22/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On July 18, 2016, an employee inadvertently misplaced a laptop with a DVD that contained a small number of investors' subscription agreements for the senior debt invested in Clear One Advantage, LLC through Clear One Funding, LP. These subscription agreements included your name, date of birth, Social Security number, contact address details, phone number, email address and investment amount.

Attribution 1 Publication: MD AG's office Author:
Article Title: Clear One Funding, LP / WWC Capital Group, LLC
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271161%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271161%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-13	Smith, Patrick LLC	MO	7/28/2016	Electronic	Business	Yes - Published #	1,649

On July 2, 2016, a principal at Smith Patrick received an email from a hacker who reported that he/she had infiltrated Smith Patrick's computer network and demanded that Smith Patrick pay a ransom. Based on Smith Patrick's investigation, the hacker entered Smith Patrick's network on or about June 17, 2016 and it is possible that certain personal information of Smith Patrick's clients may have been accessed, however, it has no way of verifying whether this has in fact occurred. Smith Patrick has determined that the information involved in this purported breach may have included the name; mailing address; social security number; and other information included on a tax return, for certain of its clients. (Consumers affected per IN AG's office)

Attribution 1 Publication: MD AG's office / IN AG's office Author:
Article Title: Smith, Patrick LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271159.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-12	SportBrella	CA	7/30/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that the section of our online store at <https://sport-brella.com> that processes customer orders was subject to an online attack, and as a result, credit card numbers, associated CVV codes, and other customer information used to make purchases in recent months may have been accessed by unauthorized parties.

Attribution 1 Publication: MD AG's office Author:
Article Title: SportBrella
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271158%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271158%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-11	Vacation Express USA Corp	GA	7/8/2016	Electronic	Business	Yes - Unknown #	Unknown

On 6/14/16, we learned that a former Vacation Express employee had been arrested. At the time of the arrest, the former employee had in his possession a small number of customers' payment card information, including your name, address, payment card number ending in XXXX, card expiration date and CVV code.

Attribution 1 Publication: MD AG's office Author:
Article Title: Vacation Express USA Corp
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271764.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-10	Water Environment Federation / Comnet	VA	7/8/2016	Electronic	Business	Yes - Unknown #	Unknown

On June 27, 2016, Comnet informed WEF that an unauthorized individual gained access to Comnet's system on April 24, 2016 and deleted the information that Comnet had collected from WEF members for membership renewals from August 17, 2015 to April 24, 2016. Comnet assisted WEF with membership renewal outreach, and stored your name, address, phone number, and payment card information when you renewed your membership through them.

Attribution 1 Publication: MD AG's office Author:
Article Title: Water Environment Federation / Comnet Marketing Group
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271765%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271765%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-09	John J. Capelli, CPA	CA	7/8/2016	Electronic	Business	Yes - Unknown #	Unknown

On May 28, 2016, I was informed that some of my clients had received a fraudulent 'DocuSign' email from me. Having no knowledge nor authorization of the 'DocuSign' email, I immediately changed my email account password, and changed email accounts. If you are an individual, this information may have included your name, gender, date of birth, telephone number, address, social security number, all employment (W-2) information, and direct deposit bank account information including account number(s) and routing information (if sent to me via email).

Attribution 1 Publication: MD AG's office Author:
Article Title: John J. Capelli, CPA
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271766.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-08	Wyndham Vacation Resorts	NJ	7/6/2016	Electronic	Business	Yes - Unknown #	Unknown

While we take reasonable steps to protect our records, on or about April 21, 2016, your owner contract was scheduled for pick up from U.S. Bank (one of our service providers) by UPS for shipment to our Las Vegas office. The package has yet to arrive at our Las Vegas office and is considered missing. This contract contained your personal information such as your name, address, Social Security number, bank account number and possibly your credit score information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Wyndham Vacation Resorts
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271769%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271769%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-07	KRT CPAs	GA	7/1/2016	Electronic	Business	Yes - Published #	3,793

We have recently learned that on April 10, 2016, our computer system was compromised by an outside attacker who was able to gain access to our tax software. While we do not believe that any fraudulent tax returns were filed using our system, our investigation indicates that the unauthorized person did have access to the data in our system during this time. (Consumers affected per IN AG's office)

Attribution 1 Publication: MD AG's office / SC AG's office / IN AG' Author:
Article Title: KRT CPAs
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271770.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-06	Frank Day, CPA LLC	NY	6/8/2016	Electronic	Business	Yes - Unknown #	Unknown

take to protect your information, and resources I am making available to help you protect your identity. On May 3, 2016, a client informed me that their tax return was found to be in the possession of an unauthorized individual. I immediately began an investigation, with the assistance of computer experts, to determine the scope of the potential compromise and determined that an unauthorized individual may have accessed my e-mail account and additional client documents. After investigating, it appears that documents may have contained your name, address, Social Security number and/or tax information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Frank Day, CPA LLC
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271790%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271790%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-05	Remedi SeniorCare	MD	6/10/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On June 6, 2016, Remedi SeniorCare ("Remedi") became aware that, on May 16, 2016, a criminal impersonating a senior company official requested and received the personal information of a number of Remedi employees, including their Social Security numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Remedi SeniorCare
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271805%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271805%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-04	BioTime, Inc.	CA	6/14/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Our client, BioTime, Inc. and its subsidiaries ("BioTime"), on June 9, 2016, learned that a targeted "phishing" email message had been sent from outside the company to a BioTime employee that same day. Upon learning this, BioTime immediately began an internal investigation. The investigation revealed that the phishing email the employee received was designed to appear as though it had been sent by a BioTime executive and requested 2015 IRS Forms W-2.

Attribution 1 Publication: MD AG's office Author:
Article Title: BioTime, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271806.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-03	Tom McLeod Software Corps	AL	6/15/2016	Electronic	Business	Yes - Unknown #	Unknown

On June 8, 2016, TMSC discovered that it had been the victim of an email spoofing scam that resulted in a compromise of the security of employee 2015 IRS Tax Form W-2 information including employee names, addresses, Social Security numbers, and wage information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Tom McLeod Software Corps
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271812.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-02	Grand Valley State University	MI	6/17/2016	Electronic	Educational	Yes - Published #	3,198

On April 25, 2016, we learned that a package mailed to the city of Grand Rapids for tax purposes had not yet been received. We immediately began a comprehensive search with the assistance of the postal service and the city of Grand Rapids to attempt to locate the package. The package included a disc which contained tax information for our employees working and/or residing in the city of Grand Rapids, including your name, address, Social Security number and 2015 income. (Consumers affected per IN AG's office)

Attribution 1 Publication: MD AG's office / IN AG's office Author:
Article Title: Grand Valley State University
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271833.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161024-01	Tricerat, Inc.	MD	6/17/2016	Electronic	Business	Yes - Unknown #	Unknown

We were recently the victims of a social engineering scam which resulted in the exposure of your 2015 W-2 information, including your name, address, social security number and salary information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Tricerat, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271831.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161021-07	Seattle Indian Health Board	WA	10/20/2016	Electronic	Medical/Healthcare	Yes - Published #	793

The Seattle Indian Health Board experienced a security attack to an employee email account on August 10, 2016. Access to the account lasted approximately 4 hours before the Seattle Indian Health Board IT department shut down the email system. The information accessed may or may not have included patients' names, date of birth, patient ID numbers, social security numbers or other protected health information.

Attribution 1 Publication: databreaches.net / SIHB / hhs.gov / hipa Author:
Article Title: Seattle Indian Health Board notified almost 800 patients after email hack
Article URL: <https://www.databreaches.net/seattle-indian-health-board-notified-almost-800-patients-after-email-hack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161021-06	Baystate Health	MA	10/21/2016	Electronic	Medical/Healthcare	Yes - Published #	13,112

About 13,000 patients of Baystate Health may have had some of their personal information compromised, due to a "phishing" e-mail that was received by some staff members. According to a Baystate Health news release sent to 22News, the information may have included names and dates of birth, in addition to medical information, such as diagnoses and the type of treatment the patient received, and even perhaps health insurance identification numbers.

Attribution 1 Publication: databreaches.net / company website / hi Author:
Article Title: Information of 13,000 Baystate patients possibly compromised due to "phishing"
Article URL: <https://www.databreaches.net/ma-information-of-13000-baystate-patients-possibly-compromised-due-to-phishing/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161021-05	Florida Hospital Medical Group	FL	10/21/2016	Paper Data	Medical/Healthcare	Yes - Published #	6,786

In a release, the hospital said, "While transferring boxes from our storage vendor, Access, to another one of our storage vendors, Iron Mountain, we discovered on or about Aug. 17, 2016, boxes containing patient information were inadvertently misplaced."

Attribution 1 Publication: wftv.com / databreaches.net / hipaajourn Author:
Article Title: Boxes of patient information missing from Florida Hospital in Orlando
Article URL: <http://www.wftv.com/news/local/boxes-of-patient-information-missing-from-florida-hospital-in-orlando/459486261>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161021-04	Eastwood Company	PA	10/19/2016	Electronic	Business	Yes - Published #	20,929

On July 22, 2016, Eastwood learned that malicious software code may have been inserted into its e-commerce website. We immediately removed the malicious software, began an investigation and hired a third-party cybersecurity firm to assist us. Findings from the investigation show that if a customer placed an order on our website from May 29, 2016 to July 22, 2016, information associated with the order being placed, including the customer's name, address, phone number, email address, payment card number, expiration date and security code (CVV) may have been obtained by an unauthorized third-party. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / VT AG's office / WA AG Author:
Article Title: Eastwood Company
Article URL: https://oag.ca.gov/system/files/Eastwood%20CA_Redacted_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161021-03	Health Access Network / Lincoln Medical Center	ME	10/19/2016	Electronic	Medical/Healthcare	Yes - Published #	17,000

Health Access Network is warning "a very small number" of its 17,000 patients to beware of identity theft after firing a new employee for improperly accessing patient clinical information, its CEO said Wednesday. The worker had access to patient billing information — including Social Security numbers and payment arrangements — as part of her job, but she was fired after computer tracking indicated that she inappropriately opened clinical data.

Attribution 1 Publication: bangordailynews.com / hipaajournal.com Author:
Article Title: Lincoln health center warning patients of data breach, fired worker
Article URL: <http://bangordailynews.com/2016/10/19/health/lincoln-health-center-warning-patients-of-data-breach-fired-worker/?ref=>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161021-02	Foursquare	NY	10/20/2016	Electronic	Business	Yes - Unknown #	Unknown

It's not known when Foursquare, a location-based check-in site, was attacked, but the group claims more than 22.5 million accounts were stolen in the alleged breach. According to another sample given to us, each record contains an email address, first and last name, gender, their location, Facebook ID, and Twitter username.

Attribution 1 Publication: zdnet.com Author:
Article Title: Weebly confirms hack; millions of Foursquare accounts also exposed
Article URL: <http://www.zdnet.com/article/millions-of-accounts-stolen-in-weebly-foursquare-breaches/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161021-01	Weebly	CA	10/20/2016	Electronic	Business	Yes - Unknown #	Unknown

Weebly, a San Francisco-based company that has allowed more than 40 million people create websites with since 2007; will start sending notification letters to all of their customers on Thursday, informing them of a data breach that occurred eight months ago. The breach, affecting 43,430,316 customers, happened February 2016, but the root cause remains unknown

Attribution 1 Publication: CSOnline.com Author:
Article Title: Weebly data breach affects 43 million customers
Article URL: <http://www.csonline.com/article/3133031/security/weebly-data-breach-affects-43-million-customers.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161019-03	Genesis Physical Therapy	CA	10/7/2016	Electronic	Medical/Healthcare	Yes - Published #	2,245

Genesis Physical Therapy, Inc. CA Healthcare Provider 2245 10/07/2016 Unauthorized Access/Disclosure Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: Genesis Physical Therapy
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161019-02	National Republican Senatorial Committee (NRSC)	DC	10/18/2016	Electronic	Business	Yes - Unknown #	Unknown

The digital storefront used by the National Republican Senatorial Committee (NRSC) to sell products ranging from "Never Hillary" stickers to "Make America Great Again" bracelets was compromised for nearly six months starting March 16, researcher Willem de Groot wrote in a recent report. (Targeted Victory)

Attribution 1 Publication: nakedsecurity.sophos.com Author:
Article Title: Republican site rigged with credit card skimmer malware for 6 months
Article URL: <https://nakedsecurity.sophos.com/2016/10/19/republican-site-rigged-with-credit-card-skimmer-malware-for-6-months/>

Attribution 2 Publication: WashingtonTimes.com / databreaches.net Author:
Article Title: Hackers stole credit card data from Republican website for 6 months: Report
Article URL: <http://www.washingtontimes.com/news/2016/oct/18/hackers-stole-credit-card-data-from-republican-web/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161019-01	Mercy Hospital and Medical Center	IL	10/18/2016	Paper Data	Medical/Healthcare	Yes - Published #	547

On August 15, 2016, Mercy Hospital & Medical Center discovered that some medical billing information for a total of 547 patients was potentially exposed as a result of a third-party billing service's loss of Mercy's documents from their offices.

Attribution 1 Publication: databreaches.net Author:
Article Title: Mercy Hospital & Medical Center notifies patients after billing service loses 547 patients' documents
Article URL: <https://www.databreaches.net/il-mercy-hospital-medical-center-notifies-patients-after-billing-service-loses-547-patient>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-16	Delta Career Education Corporation	VA	10/13/2016	Electronic	Educational	Yes - Published #	4,014

According to the investigation, Delta believes that an unauthorized individual or individuals potentially obtained copies of all Forms W-2 that Delta sent to employees for calendar year 2015, which contain names, addresses, Social Security numbers, and income information. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: Delta Career Education Corporation
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/delta-career-20161013.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-15	Chevron USA, Inc.	CA	10/17/2016	Electronic	Business	Yes - Unknown #	Unknown

On or about June 4, 2016, Chevron noticed certain electronic files appeared to be missing. Chevron immediately began working diligently to investigate to determine what happened. On July 1, 2016, Chevron confirmed that the files were removed from their system. An internal investigation revealed a contractor working on a project copied files to a personal hard drive and took it with him after the expiration of the contract.

Attribution 1 Publication: NH AG's office Author:
Article Title: Chevron USA, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/chevron-20161012.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-14	Big Y Foods	CT	10/13/2016	Electronic	Business	Yes - Unknown #	Unknown

On or around September 29, 2016, Big Y Foods, Inc. ("Big Y") discovered, and immediately removed, "skimmers" on five (5) single-payment terminals, located in five (5) of its seventy-five (75) stores. The five (5) impacted stores are located in Avon, Connecticut;

Attribution 1 Publication: NH AG's office Author:
Article Title: Big Y Foods
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/big-y-20161013.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-13	Borden Perlman Salisbury & Kelly	NJ	10/14/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 7, 2016, we discovered that the email accounts of two Borden Perlman employees were subject to unauthorized access. We immediately launched an internal investigation and retained third-party forensic experts to assist in the investigation of the incident. We determined that while the unauthorized individual or individuals had access to the two employees' email accounts, some of your personal information may have been viewed by the unauthorized individual including your name and Social Security number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Borden Perlman Salisbury & Kelly
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/borden-perlman-20161010.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-12	Liberty Buy Sell	OR	10/17/2016	Electronic	Business	Yes - Unknown #	Unknown

We are contacting you because we have learned of a serious data security incident that occurred on approximately 9/21/2016 that involved some of your personal information. The breach involved scanned images of your photo ID that you would have provided to complete a sales transaction with Liberty Buy Sell. The information breached contained (customer names, mailing addresses, driver's license or passport #. Other information (bank account PIN, security codes, etc.) was not released.

Attribution 1 Publication: OR AG's office Author:
Article Title: Liberty Buy Sell
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1795067647>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-11	Noble House - Teton Mountain Lodge & Spa /	WA	10/14/2016	Electronic	Business	Yes - Unknown #	Unknown

Noble House Hotels & Resorts was alerted to potential suspicious activity on the payment card system for Teton Mountain Lodge & Spa and Hotel Terra on September 6, 2016, by a computer security firm Noble House engaged to examine the systems for its properties. The information potentially compromised involved data found in the magnetic stripe on payment cards, including payment card number, payment card expiration date, CVV number, and, in some instances, the payment cardholder's name.

Attribution 1 Publication: databreaches.net Author:
Article Title: Noble House Hotels & Resorts notifies guests of payment card breaches at Teton Mountain Lodge & Spa and Hotel Terra
Article URL: <https://www.databreaches.net/noble-house-hotels-resorts-notifies-guests-of-payment-card-breaches-at-teton-mountai>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-10	One Nevada Credit Union	NV	10/17/2016	Electronic	Banking/Credit/Financial	Yes - Published #	1,000

FOX5 reported that a number of credit union members told the news station that their accounts had been “wiped out,” and that members were “scrambling” to find out what happened. The report referred to the issue only as a “breach” related to debit cards. The report included a comment from one unhappy member who said he had been with the One Nevada for 12 years and would be leaving as a result of the issue.

Attribution 1 Publication: Cutoday.com Author:
Article Title: About 1,000 Members Victimized In Skimming Breach
Article URL: <http://www.cutoday.info/Fresh-Today/About-1-000-Members-Victimized-In-Skimming-Breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-09	Broadview Mortgage	CA	7/28/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On July 28, 2016, we were advised by our third-party information technology provider that it had identified two unauthorized administrative accounts on a server in one of our branch offices. We immediately began an investigation and promptly disabled the unauthorized accounts.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Broadview Mortgage
Article URL: https://oag.ca.gov/system/files/Broadview%20Adult_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-08	Office of Curtis F. Robinson, MD, Inc. / Marin Medical	CA	7/26/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On August 22, 2016, we received confirmed notice from our electronic medical record provider that their electronic system was subject to a malware attack on July 26, 2016. They became aware of the incident on July 27, 2016, and we are informed that they promptly took action to secure their systems.

Attribution 1 Publication: CA AG's office / databreaches.net Author:
Article Title: Office of Curtis F. Robinson, MD, Inc. / Marin Medical Practice Concepts
Article URL: https://oag.ca.gov/system/files/Robinson%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-07	Integrity Transitional Hospital	TX	10/17/2016	Electronic	Medical/Healthcare	Yes - Published #	29,514

Integrity Transitional Hospital of Denton, TX has discovered an unauthorized individual gained access to its computer system and potentially viewed lab test results and other sensitive patient data. The security breach affects patients of a number of different healthcare providers.

Attribution 1 Publication: hipaajournal.com / CA AG's office / VT A Author:
Article Title: Integrity Transitional Hospital Learns of Data Breach
Article URL: <http://www.hipaajournal.com/integrity-transitional-hospital-learns-of-data-breach-3634/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-06	CalOptima #2	CA	10/18/2016	Electronic	Medical/Healthcare	Yes - Published #	56,000

Prior to leaving employment, the former employee downloaded the protected health information of individuals who were enrolled in the county's health plan for low-income and disabled Californians.

Attribution 1 Publication: hipaajournal.com / CA AG's office / data Author:
Article Title: CalOptima Discovers Breach That Could Impact 56,000 Members
Article URL: <http://www.hipaajournal.com/caloptima-discovers-breach-that-could-impact-56000-members-3636/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 67 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-05	Fred's Stores of Tennessee	TN	9/29/2016	Electronic	Medical/Healthcare	Yes - Published #	9,624

In late September, Fred's Stores of Tennessee Inc., reported the theft of a laptop computer containing information relating to prescriptions. 9,624 individuals were impacted by that incident.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](http://hhs.gov/hipaajournal.com) Author:
Article Title: Recent Healthcare Data Breaches Involving the Theft of Unencrypted Devices used to Store ePHI
Article URL: <http://www.hipaajournal.com/theft-of-unencrypted-laptop-results-in-exposure-of-3100-patients-ephi/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-04	Warren Clinic	OK	10/7/2016	Electronic	Medical/Healthcare	Yes - Published #	2,938

St Francis Health System has announced that a hacker has gained access to a database used to store information of patients of the Warren Clinic; a division of St. Francis that provides primary care and specialty medical services to patients throughout Eastern Oklahoma. On September 7, 2016, a hacker made contact with St. Francis Health System demanding payment in exchange for the return of data that were stolen from one of its servers. A third party security firm was contracted to conduct a thorough investigation of the security breach which revealed a database containing health data of almost 3,000 patients had been compromised.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](http://hhs.gov/hipaajournal.com) Author:
Article Title: St. Francis Health System Announces Extortion Attempt
Article URL: <http://www.hipaajournal.com/st-francis-health-system-announces-extortion-attempt-3633/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-03	Rainbow Children's Clinic	TX	10/3/2016	Electronic	Medical/Healthcare	Yes - Published #	33,698

On August 3, 2016, a hacker gained access to the clinic's computer system and encrypted a range of data stored on its servers including the protected health information of patients. The ransomware prevented critical patient files from being accessed, which naturally had a direct impact on patients.

Attribution 1 Publication: [hhs.gov / hipaajournal.com / databreach](http://hhs.gov/hipaajournal.com/databreach) Author:
Article Title: Rainbow Children's Clinic Ransomware Attack Resulted in Data Loss
Article URL: <http://www.hipaajournal.com/rainbow-childrens-clinic-ransomware-attack-resulted-in-data-loss-3635/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-02	Peabody Retirement Community	IN	10/14/2016	Electronic	Medical/Healthcare	Yes - Published #	1,466

Peabody Retirement Community IN Healthcare Provider 1466 10/14/2016 Hacking/IT Incident Email, Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Peabody Retirement Community
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161018-01	Gibson Insurance Agency	IN	10/14/2016	Electronic	Business	Yes - Published #	7,242

On July 28, 2016, we discovered an employee's laptop computer had been stolen. We immediately conducted an investigation. It was determined the files on the laptop may have contained your name, address, date of birth, Social Security number, and health insurance information.

Attribution 1 Publication: [hhs.gov / databreaches.net / hipaajournal](http://hhs.gov/databreaches.net/hipaajournal) Author:
Article Title: Indiana business associate providing employee benefits management notifies 7,242 after laptop theft
Article URL: <https://www.databreaches.net/indiana-business-associate-providing-employee-benefits-management-notifies-7242-aft>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 68 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161017-01	Katy Independent School District / SunGard K-12	TX	10/17/2016	Electronic	Educational	Yes - Published #	78,000

SunGard K-12, a third-party student and employee data management vendor, has informed Katy ISD of a potential data exposure related to a software installation the company initiated and sent to other school districts without Katy ISD's knowledge or authorization.

Attribution 1 Publication: databreaches.net Author:
Article Title: Katy ISD notifies parents after third-party error by SunGard K-12
Article URL: <https://www.databreaches.net/tx-katy-isd-notifies-parents-after-third-party-error-by-sungard-k-12/>

Attribution 2 Publication: KHOU.com Author:
Article Title: Katy ISD notifies parents of potential data breach of students' info
Article URL: <http://www.khou.com/news/local/katy-isd-notifies-parents-of-potential-data-breach-of-students-info/336937199>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-15	Krispy Kreme Donut Corporation	NC	6/18/2016	Electronic	Business	Yes - Unknown #	Unknown

On the afternoon of June 17, 2016, Krispy Kreme Donut Corporation (KKD) was the target of a phishing attack to access employee payroll records.

Attribution 1 Publication: MD AG's office Author:
Article Title: Krispy Kreme Donut Corporation
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271849.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-14	National Church Solutions	WV	6/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On or about February 8, 2016, the Federal Bureau of Investigation ("FBI") informed NCS that it had detected a malicious IP address communicating with its network. On May 5, 2016 NCS determined that a virus infected certain devices on its systems between February 3, 2016 and February 9, 2016, and that this virus may have resulted in unauthorized access to some information related to certain businesses with which it works, including the organization's: address, phone number, bank account information and the Federal Tax Identification number.

Attribution 1 Publication: MD AG's office Author:
Article Title: National Church Solutions
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271851.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-13	Independent Medical Specialty Dealers Association	OH	6/22/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 29, 2016, a laptop owned by Select Association Management, and used by one of its employees, was stolen from a luggage storage area while at a business function at a hotel in Tennessee. Select Association Management is the management company of the Independent Medical Specialty Dealers Association ("IMDA"). Based on its internal investigation of this matter, IMDA has determined that certain emails stored on the stolen laptop may have contained individuals' names and credit card numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Independent Medical Specialty Dealers Association / Select Association Management
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271853%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271853%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-12	HSBC Securities USA, Inc.	NY	7/15/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We became aware of an incident where a former employee printed and took customer account information prior to leaving HSBC on June 8, 2016 and began contacting those customers from his new employer, Wells Fargo. The information accessible included customer name, mailing address, social security number, date of birth, e-mail address, financial account numbers and phone numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: HSBC Securities USA, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-272253.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-11	Paul Stuart	NY	6/20/2016	Electronic	Business	Yes - Unknown #	Unknown

On Tuesday, May 10, a Paul Stuart employee mistakenly responded to a phishing email by releasing confidential personally identifiable employee information. We identified the incident on June 14, and immediately proceeded to take appropriate corrective measures.

Attribution 1 Publication: Paul Stuart Author:
Article Title: Paul Stuart
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271863%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271863%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-10	Pennsylvania Lumbermens Mutual Insurance Company	PA	6/28/2016	Electronic	Business	Yes - Unknown #	Unknown

On June 16, 2016, Pennsylvania Lumbermens Mutual Insurance Company was the targeted victim of an email spoofing attack. Through this email spoofing attack, a successful request was made for 2015 current and former employees' Tax Form W-2 information to be sent to an email address purporting to be from within PLM. The information on the disclosed W-2 included your name, address, wage and tax amounts, and Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Pennsylvania Lumbermens Mutual Insurance Company
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271868.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-09	Rayner, Foos, Kruse and Irwin	OH	6/28/2016	Electronic	Business	Yes - Published #	1,336

On April 18, 2016, RFKI learned that a possible security incident may have impacted the security of information stored on its servers. RFKI immediately began an investigation and engaged independent, third-party forensic computer experts to assist. On May 27, 2016 RFKI learned from the forensic computer experts that files stored on its system may have been accessed by an unauthorized individual. These files contain information related to tax returns, including names, addresses, Social Security numbers, and possibly bank account information. (Consumers affected per IN AG's office)

Attribution 1 Publication: MD AG's office / IN AG's office / MT AG; Author:
Article Title: Rayner, Foos, Kruse and Irwin
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271871.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-08	Quikrete, Inc.	CA	6/7/2016	Electronic	Business	Yes - Unknown #	Unknown

The Company recently learned that one of its Human Resources employees inadvertently sent by email a spreadsheet containing social security numbers to area supervisors in other divisions of the Company who did not have a need for such information to perform their job functions. This spreadsheet included your name and social security number, as well as that of your dependents on your health care plan.

Attribution 1 Publication: MD AG's office Author:
Article Title: Quikrete, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271926.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-07	Higdon & Hale Certified Public Accountants	KS	6/23/2016	Electronic	Business	Yes - Unknown #	Unknown

It is our understanding that on approximately May 14, 2016, an unknown cyber attacker gained improper access into the firm's computer systems and appears to have accessed numerous client files. The cyber hacker appears to have again improperly accessed the systems on May 11th, attempting to again obtain and misuse information on the firm's current and former clients.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Higdon & Hale
 Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271934%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271934%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-06	Flynn & Company, Inc. Certified Public Accountants	OH	6/27/2016	Electronic	Business	Yes - Unknown #	Unknown

On May 26, 2016, the forensic investigation concluded that, beginning on March 1, 2016, a foreign third-party had gained unauthorized access to our systems, which are outsourced and managed by our third-party IT provider, and could have viewed or acquired certain files containing client information. We can confirm that the files that may have been accessed contained your full name and Social Security number.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Flynn & Company, Inc. Certified Public Accountants
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-271935.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-05	Washington County Housing and Redevelopment Authority	MD	6/23/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 14, 2016, we discovered that on that same day, as a result of a sophisticated network intrusion, an unauthorized third party gained access to one of our servers. Upon learning of the issue, our incident response team promptly launched an investigation and notified local law enforcement. Because we value our relationship with you, we wanted to make you aware of this incident because the unauthorized party may have accessed some of your personal information within the infected server, including your full name and < Alt Address (Social Security number; driver's license number; bank account information)>.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Washington County Housing and Redevelopment Authority
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-272236.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-04	Santander	MA	7/12/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On June 23, 2016 the Santander Bank Fraud Card Detection group discovered suspicious ATM withdrawals. Upon further investigation, it was determined that a magnetic stripe skimming device had been placed on the ATM vestibule door of our ATM located at 901 West Park Avenue, Ocean, New Jersey. After reviewing video surveillance footage, it was determined that the device had been placed on the ATM vestibule door on May 6, 2016 and removed May 8, 2016. Furthermore, a camera device was installed in the ATM Light Lens. The personal information potentially compromised included the customer's name, card number, card expiration date, card security code, and card PIN number.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Santander
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-272249.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-03	Virginia Premier Health Plan	VA	7/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 11, 2016 we discovered that on June 30, 2016, as a result of a complex phishing incident, an unauthorized third party obtained an electronic file containing certain information on current and former employees who received employment earnings in 2015 from VPHP.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Virginia Premier Health Plan
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-272257.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-02	Hogan Taylor, LLP	OK	7/29/2016	Electronic	Business	Yes - Unknown #	Unknown

Hogan Taylor has recently learned that, on June 28, 2016, during the audit of a company's benefit plan, a member of our firm mistakenly forwarded an email containing names and Social Security numbers to a wrong party instead of to the benefit plan administrator, as was necessary for our audit. While Hogan Taylor does not believe that information was disclosed any further or used for any improper purpose, out of an abundance of caution, it is notifying every person affected by this incident.

Attribution 1 Publication: MD AG's office Author:
Article Title: Hogan Taylor, LLP
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-272311.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161014-01	TD Bank / Santander	MA	8/4/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

As you may be aware already, on February 25, 2016, Santander Bank, N.A. sent an image cash letter file to the Federal Reserve Bank (FRB). The file did not have correct alignment of the data to the image records and as a result, it is possible that check images from the file were viewed by third parties (i.e. unintended recipients of the check image). The personal information viewed may have been name, address and account number.

Attribution 1 Publication: NH AG's office Author:
Article Title: TD Bank / Santander
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/td-bank-20160804.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-24	TD Bank	NJ	10/4/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently learned that one of our employees inappropriately obtained and used confidential customer information which may have resulted in fraudulent activity on their account. The personal information which was exposed may have included name, address, date of birth, social security number, and account number.

Attribution 1 Publication: NH AG's office Author:
Article Title: TD Bank
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/td-bank-20161004.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-23	MicroDAQ	NH	10/11/2016	Electronic	Business	Yes - Unknown #	Unknown

MicroDAQ has learned that an unknown third party imbedded malware onto MicroDAQ's website that caused some customers' financial information to be sent surreptitiously to an email account not associated with MicroDAQ as orders were placed online. The customers affected could include those who purchased products from our website, www.MicroDAO.com, between September 4 and September 22, 2016.

Attribution 1 Publication: NH AG's office Author:
Article Title: MicroDAQ
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/microdaq-20161007.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-22	HD Vest Investment Services	TX	10/5/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On August 1, 2016, HD Vest learned that Patricia Flagg, an HD Vest Advisor, received a message on her computer that it was infected with a virus and provided her with a contact number for assistance in removing the virus. Suspicious of the incident, Ms. Flagg notified HD Vest. HD Vest immediately began an investigation and learned that, while the unauthorized person was connected to Ms. Flagg's computer, the unauthorized person would have had access to certain individuals' information accessible from the computer.

Attribution 1 Publication: NH AG's office Author:
Article Title: HD Vest Investment Services
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/hd-vest-investment-20161005.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-21	New Horizons Computer Learning Centers South	FL	10/6/2016	Electronic	Educational	Yes - Unknown #	Unknown

On August 22, 2016, New Horizons discovered an unauthorized individual had gained access to its network. New Horizons immediately took action to secure its system and conducted an investigation to determine what information that individual may have gained access to. New Horizons determined that some files may have contained employee and student information, including names, addresses, Social Security numbers, and email addresses.

Attribution 1 Publication: NH AG's office Author:
 Article Title: New Horizons Computer Learning Centers South Florida
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/geb-computer-training-20161006.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-20	Office of Francisco Jaime, D.O.	AZ	10/4/2016	Electronic	Medical/Healthcare	Yes - Published #	14,236

Francisco Jaime, D.O. AZ Healthcare Provider 14236 10/04/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov / IN AG's office Author:
 Article Title: Office of Francisco Jaime, D.O.
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-19	Baxter Regional Medical Center - Home Health Facility	AR	10/5/2016	Paper Data	Medical/Healthcare	Yes - Published #	2,124

Baxter Regional Home Health is alerting patients to a potential breach of their protected health information following a break-in at its facility in Cotter, Arkansas. The break-in occurred during the night and was discovered on August 5, 2016.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
 Article Title: BAXTER REGIONAL HOME HEALTH ALERTS PATIENTS TO POTENTIAL PHI EXPOSURE
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-18	Baxter Healthcare	IL	10/10/2016	Electronic	Medical/Healthcare	Yes - Published #	992

Illinois-based Baxter Healthcare has informed patients of a privacy breach that exposed their email addresses to members of the Patient Advisory Council. On September 15, 2016, an employee sent an email to 992 patients inviting them to take part in the Patient Advisory Council.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
 Article Title: Baxter Healthcare
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-17	Apria Healthcare	CA	10/5/2016	Electronic	Medical/Healthcare	Yes - Published #	1,987

On August 5, 2016, Apria Healthcare discovered that the email account of an Apria Healthcare employee was subject to unauthorized access and immediately launched an internal investigation and retained third-party forensic experts to assist in the investigation of the incident. The forensic investigators later determined that the email account contained the personal information of certain individuals. Apria Healthcare then undertook a thorough analysis and review of all documents within the email account to determine all affected individuals and data types involved.

Attribution 1 Publication: databreaches.net / hhs.gov / CA AG's of Author:
 Article Title: Apria Healthcare notifies patients of breach
 Article URL: <https://www.databreaches.net/ca-apria-healthcare-notifies-patients-of-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-16	Marin Healthcare District / Marin Medical Practices	CA	10/6/2016	Electronic	Medical/Healthcare	Yes - Published #	2,292
<p>Marin Medical Practices Concepts, Inc., (MMPC) provides a range of business and health care system services for Marin Healthcare District. On July 26, 2016 MMPC discovered that ransomware had been installed on its system preventing access to critical files. (records per hhs.gov)</p>							

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
 Article Title: HEALTHCARE VENDOR PAYS RANSOM AFTER BACKUP SYSTEM FAILURE
 Article URL: <http://www.hipaajournal.com/healthcare-vendor-pays-ransom-backup-system-failure-3622/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-15	Thomasville Eye Center	GA	10/10/2016	Electronic	Medical/Healthcare	Yes - Published #	10,891
<p>A former employee of the Thomasville Eye Center in Thomasville, GA has been discovered to have accessed the protected health information of patients without authorization. PHI was stolen from the eye center and used to open credit accounts in the names of the patients.</p>							

Attribution 1 Publication: hipaajournal.com Author:
 Article Title: GEORGIA EYE CENTER DISCOVERS INSIDER BREACH: 10,891 PATIENTS IMPACTED
 Article URL: <http://www.hipaajournal.com/georgia-eye-center-discovers-insider-breach-10891-patients-impacted-3626/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-14	VA Department of Veterans Services / McGuire VA	VA	10/11/2016	Paper Data	Government/Military	Yes - Published #	5,051
<p>The Virginia Department of Veterans Services (DVS) has launched an investigation following the discovery of 20-30 boxes of files in an abandoned storage unit. The files contain a range of documents including unfiled claims and veterans' medical records.</p>							

Attribution 1 Publication: databreaches.net / richmond.com Author:
 Article Title: 5,051 records with personal info of Virginia vets discovered in fired ex-Veteran Services employee's storage unit
 Article URL: http://www.richmond.com/news/local/central-virginia/article_5a9caf23-fba6-5971-96fd-5c150604e7bb.html

Attribution 2 Publication: hipaajournal.com Author:
 Article Title: BOXES OF ABANDONED VETERANS SERVICES' FILES DISCOVERED
 Article URL: <http://www.hipaajournal.com/boxes-of-abandoned-veterans-services-files-discovered-3627/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-13	Peachtree Orthopedics	GA	10/13/2016	Electronic	Medical/Healthcare	Yes - Published #	531,000
<p>On September 22, 2016, the orthopedic clinic discovered that its computer systems had been accessed by an unauthorized individual who gained access to a patient database. Computer forensics experts have been brought in to conduct the investigation, which is still ongoing. The Federal Bureau of Investigation has also been notified of the security breach and investigation has been launched.</p>							

Attribution 1 Publication: hipaajournal.com / databreaches.net / V Author:
 Article Title: PEACHTREE ORTHOPEDICS DISCOVERS PATIENT DATABASE WAS HACKED
 Article URL: <http://www.hipaajournal.com/peachtree-orthopedics-discovers-patient-database-was-hacked-3630/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-12	University of Wisconsin HealthCenter	WI	10/10/2016	Paper Data	Medical/Healthcare	Yes - Published #	6,923
<p>Madison-based University of Wisconsin Health is notifying patients of a data breach after mistakenly sending patient satisfaction surveys to some patients' parents instead of the patients themselves. d Aug. 2. While the envelopes were addressed to the parents or guardians of patients, the cover letter was accurately addressed to the patient. The patient surveys included the name of the provider who treated the patient.</p>							

Attribution 1 Publication: beckershospitalreview.com / hhs.gov Author:
 Article Title: University of Wisconsin Health data breach stems from mailing error
 Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/university-of-wisconsin-health-data-breach->

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-11	Northwest Community Hospital / R-C Healthcare	IL	10/10/2016	Electronic	Medical/Healthcare	Yes - Published #	540

It may seem like old news to you by now, but some patients affected by a third-party breach at R-C Healthcare are first finding out about it now. Now Northwest Community Hospital in Arlington Heights is notifying 550 patients. They say they were first notified by R-C Healthcare on August 1.

Attribution 1 Publication: [databreaches.net / hhs.gov](#) Author:
Article Title: Northwest Community notifies patients of R-C Healthcare breach
Article URL: <https://www.databreaches.net/northwest-community-notifies-patients-of-r-c-healthcare-breach/>

Attribution 2 Publication: [beckershospitalreview.com](#) Author:
Article Title: Vendor data breach affects 550 Northwest Community Hospital patients
Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/vendor-data-breach-affects-550-northwest-c>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-10	Hutchinson Community Foundation	KS	10/11/2016	Electronic	Business	Yes - Published #	5,500

On September 19, officials at the foundation found ransomware on the foundation's network server after clicking on a file and finding its contents encrypted. Upon further investigation they found that intruders had done more than infect their files with ransomware and had actually made it into the foundation's systems.

Attribution 1 Publication: [Scmagazine.com](#) Author: Robert Abel
Article Title: Data breach and ransomware hit Hutchinson Community Foundation
Article URL: <http://www.scmagazine.com/data-breach-and-ransomware-hit-hutchinson-community-foundation/article/546824/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-09	Presnell Gage, PLLC	ID	8/30/2016	Electronic	Business	Yes - Published #	8,724

Presnell Gage recently learned that a number of its clients had tax returns filed in their names without their authorization. It immediately investigated whether its information system had been accessed without authorization. On August 18, 2016 it determined that client files may have been accessed without authorization between July 16, 2016 and August 18, 2016. (Consumers affected per IN AG's office)

Attribution 1 Publication: WA AG's office / IN AG's office Author:
Article Title: Presnell Gage, PLLC
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/PresnellGagePLLC.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-08	Group Health Cooperative	WA	9/23/2016	Paper Data	Medical/Healthcare	Yes - Published #	668

On September 6, 2016, Group Health Cooperative discovered a potential privacy breach related to a letter notifying the member of their coverage termination. Letters mailed on August 31, 2016, September 1, 2016 and September 2, 2016 was sent to the wrong subscriber. The member information on the letter included: patient name, address, and medical record number. No financial data, Social Security number, or medical information was included.

Attribution 1 Publication: WA AG's office / hhs.gov Author:
Article Title: Group Health Cooperative
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/GroupHealthCoop

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-07	Vermont Health Connect / WEX / Samanage	CT	10/7/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Just recently, we were informed by Samanage Ltd., our subcontractor, that a data file containing your Personal Information inadvertently may have become accessible in an unauthorized manner. Samanage provides information technology support functions under a contract to us. We are a service provider for the State of Vermont. From the information provided to us by Samanage, this data file may have been accessible between June 2, 2016 and July 27, 2016.

Attribution 1 Publication: VT AG's office / databreaches.net Author:
 Article Title: Vermont Health Connect / WEX / Samanage
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Wex%20Health%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-05	Vaupell	WA	10/3/2016	Electronic	Business	Yes - Published #	2,897

We write to you with important information about a potential compromise of certain personal information that occurred on the evening of September 12, 2016. On that date, an unauthorized person accessed our internal network servers for approximately 37 minutes, some portion of which was spent accessing a departmental server. The drives accessible to the intruder on that server included some small number of files containing personal information, including your personal information. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / WA AG Author:
 Article Title: Vaupell
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Vaupell%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-04	Vera Bradley, Inc.	IN	7/25/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 15, 2016, Vera Bradley was provided information from law enforcement regarding a potential data security issue related to our retail store network. Upon learning this information, Vera Bradley immediately launched an investigation with the assistance of a leading computer security firm to aggressively gather facts and determine the scope of the issue and promptly notified the payment card networks. Findings from the investigation show unauthorized access to Vera Bradley's payment processing system and the installation of a program that looked for payment card data

Attribution 1 Publication: CA AG's letter / eSecurityplanet.com Author:
 Article Title: Vera Bradley, Inc.
 Article URL: https://oag.ca.gov/system/files/Regulatory%20Packet%20%28CA%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-03	Qvale Auto Group, Inc.	CA	10/7/2016	Electronic	Business	Yes - Unknown #	Unknown

The incident occurred when, during the course of an upgrade by a third party IT vendor, employee access limitations were removed to certain information of employees for a limited time period in June 2016. This allowed certain employees to potentially access that information. As soon as this error was discovered, it was corrected.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Qvale Auto Group, Inc.
 Article URL: https://oag.ca.gov/system/files/Qvale%20Notification%20%2810-7-16%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-02	Public Health Institute	CA	10/5/2016	Electronic	Business	Yes - Unknown #	Unknown

We are writing to let you know about a data incident in which a database containing your personal information was accessible on the internet without encryption or other security features. The California Environmental Health Tracking Program (CEHTP) of the Public Health Institute (PHI) became aware on August 4, 2016 that an electronic database containing email addresses and corresponding passwords for individual user accounts at one or more of the sites listed below was accessible on the internet without encryption or other security features for approximately 30 days.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Public Health Institute
 Article URL: https://oag.ca.gov/system/files/1887.2%20Notice%20of%20Data%20Breach%20PHI%20CEHTP%20final%20100516_0.p

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 76 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161013-01	Office of Hal Meadows, MD	CA	9/8/2016	Electronic	Medical/Healthcare	Yes - Published #	6,000

On July 27, 2016, Dr. Meadows found that his patient file had been unlawfully accessed. The patient file contained information used for billing, which included:

Names and addresses, Birth dates, Telephone numbers, Insurance numbers, Treatment codes, and Billing information

Attribution 1 Publication: CA AG's office / hipaajournal.com / hhs. Author:
Article Title: Office of Hal Meadows, MD
Article URL: https://oag.ca.gov/system/files/meadows%20notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-11	Prima Medical Foundation / Marin Medical Practices	CA	9/30/2016	Electronic	Medical/Healthcare	Yes - Published #	Unknown

On July 26, 2016, Prima Medical Foundation, the Foundation that supports the Prima Medical Group, a local, physician owned and operated group of physicians dedicated to providing high-quality care throughout Marin, Sonoma, and Napa counties, received notice that Marin Medical Practices Concepts, Inc., (MMPC), the company that provides Prima with business and health care system services, experienced a ransomware infection. (records per hhs.gov)

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: UPDATE: 5,000 Marin Medical Practices Concepts patient records lost during recovery from ransomware attack
Article URL: <https://www.databreaches.net/update-5000-marin-medical-practices-concepts-patient-records-lost-during-recovery-fro>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-10	VF Outlet, Inc.	NC	9/27/2016	Electronic	Business	Yes - Unknown #	Unknown

Specifically, on August 18, 2016, we found indication that an unauthorized individual accessed a third party computer server that hosted the VF Outlet website (www.vfoutlet.com). Through our subsequent investigation, we learned that personal information of customers of the vfoutlet.com website may have been accessed by a third party between April 17, 20 16 and August 26, 20 16, when we shut down the website. W

Attribution 1 Publication: NH AG's office Author:
Article Title: VF Outlet, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/vf-outlet-20160927.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-09	Urgent Care Clinic of Oxford	MS	10/4/2016	Electronic	Medical/Healthcare	Yes - Published #	64,000

Urgent Care Clinic of Oxford, MS has notified its patients that their protected health information may have been viewed by unauthorized individuals after malicious actors gained access to a computer server in July 2016. Data stored on the server included names, social security numbers, birthdates, personal information, and health information.

Attribution 1 Publication: hipaajournal.com / databreaches.net / h Author:
Article Title: URGENT CARE CLINIC OF OXFORD NOTIFY PATIENTS OF HACKING INCIDENT
Article URL: <http://www.hipaajournal.com/urgent-care-clinic-of-oxford-notify-patients-of-hacking-incident-3618/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-08	US Public Health Service Commissioned Corps	DC	10/4/2016	Electronic	Government/Military	Yes - Published #	6,600

Another federal agency has experienced a breach of personal information, this time, the data of current, former, and retired members of the United States Public Health Service Commissioned Corps has been compromised. According to the Washington Post, the Commission learned of the breach on September 20. A system used to "process payroll, leave, time, attendance, and other functions" appears to have been accessed by unauthenticated users.

Attribution 1 Publication: hipaajournal.com / databreaches.net Author:
Article Title: SURGEON GENERAL WARNS EMPLOYEES OF PERSONAL INFORMATION BREACH
Article URL: <http://www.hipaajournal.com/surgeon-general-warns-employees-personal-information-breach-3619/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 77 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-07	Willow Bend Dental	TX	8/31/2016	Electronic	Medical/Healthcare	Yes - Published #	625

Willow Bend Dental TX Healthcare Provider 625 08/31/2016 Theft Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Willow Bend Dental
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-06	Santa Cruz County Health Services Agency	CA	9/2/2016	Paper Data	Government/Military	Yes - Published #	25,000

Santa Cruz County Health Services Agency CA Healthcare Provider 2500 009/02/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Santa Cruz County Health Services Agency
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-05	San Juan Oncology Associates	NM	9/29/2016	Electronic	Medical/Healthcare	Yes - Published #	500

San Juan Oncology Associates NM Healthcare Provider 500 09/29/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: San Juan Oncology Associates
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-04	McLaren Greater Lansing Cardiovascular Group	MI	9/21/2016	Electronic	Medical/Healthcare	Yes - Published #	1,000

McLaren Greater Lansing Cardiovascular Group MI Healthcare Provider 1000 09/21/2016 Unauthorized Access/Disclosure Desktop Computer, Electronic Medical Record, Other

Attribution 1 Publication: hhs.gov Author:
Article Title: McLaren Greater Lansing Cardiovascular Group
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-03	Jennie Stuart Medical Center	KY	9/23/2016	Electronic	Medical/Healthcare	Yes - Published #	1,500

Jennie Stuart Medical Center KY Healthcare Provider 1500 09/23/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Jennie Stuart Medical Center
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-02	Heritage Medical Partners	SC	9/15/2016	Paper Data	Medical/Healthcare	Yes - Published #	812

Heritage Medical Partners, LLC SC Healthcare Provider 812 09/15/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Heritage Medical Partners
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20161004-01	Winston Dillard School District No. 116	OR	10/3/2016	Electronic	Educational	Yes - Unknown #	Unknown

You are receiving this letter because of recent incidents which appear to potentially breach the security of a database holding personally identifiable information used in accounting procedures by Winston Dillard School District No. 116 for employees and former employees. This access, which appears to have occurred on three occasions, may have exposed your personally identifiable information to potential identity theft by unauthorized viewing or download of data containing your name, address, social security number, financial account number, insurance number and company, and date of birth.

Attribution 1 Publication: OR AG's office Author:
Article Title: Winston Dillard School Distric No. 116
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/732829402>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160929-07	Florida Bar Association	FL	9/25/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 22, a hacker or hackers associated with a former Palm Beach County Sheriff's Office deputy, who has a long-standing dispute with Florida law enforcement that appears to have gotten him raided by the FBI, managed to access and acquire what appears to be their entire database.

Attribution 1 Publication: databreaches.net Author:
Article Title: Florida Bar Association hacked, members' data leaked (UPDATE3)
Article URL: <https://www.databreaches.net/florida-bar-association-hacked-members-data-leaked/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160929-06	Mastic Beach	NY	9/27/2016	Electronic	Government/Military	Yes - Published #	488

The village of Mastic Beach says 488 residents may have had their personal information stolen in a data breach by a former employee pretending to be the chief of police. Mayor Maura Sperry says an 18-month audit discovered a former village employee illegally accessed highly personal information from a law enforcement database.

Attribution 1 Publication: databreaches.net Author:
Article Title: 488 affected by data breach in Mastic Beach
Article URL: <http://longisland.news12.com/news/488-affected-by-data-breach-in-mastic-beach-1.12376103>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160929-05	Habitat for Humanity of Colorado	CO	9/29/2016	Electronic	Business	Yes - Unknown #	Unknown

For the past several months, HFHC has been dealing with a significant and malicious data breach which has severely handicapped our ability to efficiently conduct business and has hijacked our attention for the last several months. Compromised personal information is limited only to documents that included first and last name, address, date of birth, and either a social security number or driver's license number. At this time we believe this only includes HFHC staff and applicants specific to USDA loans and FHLB subsidies.

Attribution 1 Publication: databreaches.net / HFHC website Author:
Article Title: Habitat for Humanity Colorado discloses severely handicapping data breach
Article URL: <https://www.databreaches.net/habitat-for-humanity-colorado-discloses-severely-handicapping-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160929-04	New Jersey Spine Center	NJ	9/22/2016	Electronic	Medical/Healthcare	Yes - Published #	28,308

On July 27, 2016, our computer systems were attacked by a malware ransom virus called "CryptoWall." The malware was detected by our virus protection software but unfortunately not until after our electronic patient records were encrypted. The virus encrypted, thereby rendering unusable, all of our electronic medical record files that contained all of the clinical information on our patients such as procedures, office notes, reports, etc. In addition to the medical information, the records contained demographic information such as date of birth, address, and in some cases SSN, credit card and account information.

Attribution 1 Publication: OR AG's office / databreaches.net / hhs. Author:
 Article Title: New Jersey Spine Center
 Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1818074805>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160929-03	Santoro CPA / Simplebooks Corp.	CT	9/27/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 19, 2016, the forensic investigators informed us that an unauthorized user may have accessed the data housed on Santoro CPA's server. This includes information related to tax documents and bookkeeping records that may have included your name, address, and Social Security number.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
 Article Title: Santoro CPA / Simplebooks Corp.
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Santoro%20CPA%20and%20Simplebooks%20Corp%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160929-02	Vermont Health Connect #1	VT	9/21/2016	Electronic	Medical/Healthcare	Yes - Published #	700

It has come to our attention that some of your fair hearing discovery documents were inadvertently mailed to the wrong petitioner. On September 13th, VHC discovered that a legal assistant inadvertently mailed documents containing case notes, notices, and payment information to another VHC consumer.

Attribution 1 Publication: VT AG's office / timesargus.com / databr Author:
 Article Title: Vermont Health Connect
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Vermont%20Health%20Connect%20SBN%20to%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160929-01	Producteev / Jive Software	CA	9/23/2016	Electronic	Business	Yes - Unknown #	Unknown

We learned on August 24 that your Producteev username and password had been held in a file outside our normal encryption procedures, and we believe that this file was potentially accessed by an unauthorized third party. We cannot confirm that your username or password was compromised, but we are notifying you so that you may take protective action.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Producteev / Jive Software
 Article URL: https://oag.ca.gov/system/files/2016-09-23%20All%20User%20Email%20Notice_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160927-04	Tully Automotive Group	NH	9/22/2016	Electronic	Business	Yes - Unknown #	Unknown

Please be advised that on September 19, 2016, Tully Automotive Group ("Company") learned that an unauthorized person improperly accessed the payroll records of certain employees stored on its payroll vendor's (Paylocity's) systems.

Attribution 1 Publication: NH AG's office Author:
 Article Title: Tully Automotive Group
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/tulley-automotive-20160922.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160927-03	Scentlok Technologies	MI	9/20/2016	Electronic	Business	Yes - Published #	1,202

On or about August 31, 2016, we learned that a malware program had infected the ScentLok website and may have intercepted credit card information relating to transactions made on the ScentLok website between August 3, 2016 and August 31, 2016 namely, card number, expiration date and CVV code, and billing address (name and address, e-mail address and telephone number). (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / VT AG's office / IN AG's Author:
Article Title: Scentlok Technologies
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/scentlok-20160920.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160927-02	Specialty Equipment Market Association (SEMA) / Comnet	NJ	7/26/2016	Electronic	Business	Yes - Published #	490

SEMA learned on June 27, 2016, that one of its vendors, Comnet Marketing Group, Inc. ("Comnet"), had been the victim of a potential computer intrusion. An unauthorized user gained administrative access to Comnet's systems on April 23-24, 2016, and issued commands to delete all the data housed on Comnet's servers. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: Specialty Equipment Market Association (SEMA) / Comnet Marketing Group
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/specialty-equipment-20160726.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160927-01	Public Education Employees' Health Insurance Plan	AL	9/9/2016	Electronic	Medical/Healthcare	Yes - Published #	1,349

Public Education Employees' Health Insurance Plan AL Health Plan 1349 09/09/2016 Unauthorized Access/Disclosure Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Public Education Employees' Health Insurance Plan
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160926-01	Novation Settlement Solutions	FL	9/26/2016	Electronic	Business	Yes - Published #	Unknown

In late August, Novation learned that some of its confidential information may be in the possession of an unidentified third-party. Novation promptly initiated a fact-gathering process and, subsequently, on September 8, 2016, determined that an unidentified third-party was likely in possession of a set of Novation files including applications and contracts. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / VT AG' Author:
Article Title: Novation Settlement Solutions
Article URL: https://oag.ca.gov/system/files/Novation%20Ad%20CA%20r2prf_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-14	Freddie Mac	VA	9/16/2016	Electronic	Banking/Credit/Financial	Yes - Published #	2,361

In April 2014, Freddie Mac learned from law enforcement that in April 2013, a person or persons had unauthorized access to certain Freddie Mac Pension Plan information. The Plan information included several Plan participants' names, addresses, Social Security Numbers, dates of birth, and plan status. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: Freddie Mac
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/freddie-mac-20160919.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-13	EMR4all, Inc. / Rehab Billing Solutions	CA	9/22/2016	Electronic	Business	Yes - Unknown #	Unknown

EMR4all, Inc. was a California business providing free EMR software to physical therapy, speech therapy, and occupational therapy practices that used their associated patient billing service, Rehab Billing Solutions (RBS). Over the summer, they began shutting down operations and notifying their clients of their closure. Their effort to make a graceful exit wound up marred by a data leak that potentially impacts tens of thousands of patients and almost 30 clinics.

Attribution 1 Publication: databreaches.net Author:
Article Title: Dozens of clinics, thousands of patients impacted by third-party data leak
Article URL: <https://www.databreaches.net/dozens-of-clinics-thousands-of-patients-impacted-by-third-party-data-leak/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-12	Regpack / BlueSnap	CA	9/21/2016	Electronic	Business	Yes - Unknown #	Unknown

"Regpack has confirmed that all payments information passed to the payment processor is encrypted on its databases. Nonetheless, periodically, this information is decrypted and kept internally for analysis purposes. We identified that a human error caused those decrypted files to be exposed to a public facing server and this was the source of the data loss. This was identified by our teams going back and reviewing some of the log files as indicated in the blog discussion post. We have changed our approach to handling this data and are confident that this one-time mistake will not occur again."

- Attribution 1** Publication: securityweek.com Author:
 Article Title: 320,000 Financial Records Apparently Stolen From Payment Processor
 Article URL: <http://www.securityweek.com/320000-financial-records-apparently-stolen-payment-processor>
- Attribution 2** Publication: scmagazine.com Author:
 Article Title: BlueSnap / Regpack
 Article URL: <http://www.scmagazine.com/324k-regpack-users-info-compromised-when-decrypted-files-placed-on-public-facing-ser>
- Attribution 3** Publication: Softpedia Author: Catalin Cimpanu
 Article Title: Mystery Surrounds Possible BlueSnap Data Breach
 Article URL: <http://news.softpedia.com/news/mystery-surrounds-possible-bluesnap-data-breach-508314.shtml>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-11	Martin Army Community Hospital	GA	9/9/2016	Paper Data	Government/Military	Yes - Published #	1,000

Fort Benning, Ga.-based Martin Army Community Hospital officials are alerting all patients who received care at the hospital from January 2011 to December 2013 of a possible HIPAA breach, according to the Ledger-Enquirer. The former employee was allegedly a member of a tax fraud ring that used sensitive information gathered from discarded lab specimen labels to file fraudulent tax returns with the IRS. The former employee allegedly acquired protected health information from the labels, including names, dates of birth and Social Security numbers. Officials are unsure of how many labels were taken and how much information was used, according to the article.

- Attribution 1** Publication: hhs.gov / Beckershospitalreview.com/hip Author:
 Article Title: Martin Army Community Hospital
 Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/hospital-officials-note-possible-hipaa-breac>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-09	Asante Health System	OR	9/9/2016	Electronic	Medical/Healthcare	Yes - Published #	2,400

On July 13, 2016, we determined that an employee had inappropriately accessed certain Asante electronic patient records. A final audit of the employee's actions showed that the employee inappropriately accessed records from August 18, 2014 to July 21, 2016 that may have included your name, date of birth, medical record number, medications, diagnosis, and lab results.

- Attribution 1** Publication: hhs.gov / OR AG's office / OR AG's offic Author:
 Article Title: Asante Health System
 Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1890743510>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-08	Codman Square Health Center	MA	9/12/2016	Electronic	Medical/Healthcare	Yes - Published #	3,840

Codman Square Health Center in Dorchester, Mass has reported that an unauthorized individual gained access to the protected health information of certain patients. The data were improperly accessed via the New England Healthcare Exchange Network (NEHEN).

- Attribution 1** Publication: hhs.gov / hipaajournal.com Author:
 Article Title: PHI IMPROPERLY ACCESSED VIA NEW ENGLAND HEALTHCARE EXCHANGE NETWORK
 Article URL: <http://www.hipaajournal.com/phi-improperly-accessed-via-new-england-healthcare-exchange-network-3603/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 82 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-07	Office of Hal Meadows, M.D.	CA	7/27/2016	Electronic	Medical/Healthcare	Yes - Published #	6,000

On July 27, 2016, Dr. Meadows found that his patient file had been unlawfully accessed. The patient file contained information used for billing, which included:

Names and addresses, Birth dates, Telephone numbers, Insurance numbers, Treatment codes, and Billing information

Attribution 1 Publication: CA AG's office / hhs.gov Author:
 Article Title: Office of Hal Meadows, M.D.
 Article URL: https://oag.ca.gov/system/files/meadows%20notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-06	Premier America Credit Union	CA	6/29/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently learned that a departing employee of Premier America emailed to his non-Premier America account lists that reflected some of your personal information, in violation of our company policies, during late June 2016. Only limited personal information was included on the lists that were involved in this incident. Such personal information may include your name, address, and either your social security number or employer identification number (whichever you had on file with us in relation to the services provided by our TOP Premium Finance division).

Attribution 1 Publication: CA AG's office Author:
 Article Title: Premier America Credit Union
 Article URL: https://oag.ca.gov/system/files/FinalLetterPackage_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-05	Napa Valley Dentistry	CA	8/11/2016	Electronic	Medical/Healthcare	Yes - Published #	4,262

On August 11, 2016 we discovered that we were the victims of the theft of a password protected server that contained your personal information. The information included names, addresses, dates of birth, Social Security numbers and dental insurance information.

Attribution 1 Publication: CA AG's office / databreaches.net Author:
 Article Title: Napa Valley Dentistry
 Article URL: https://oag.ca.gov/system/files/Napa%20Valley%20Dentistry%20NOTICE%20ONLY_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-04	Yahoo	CA	9/22/2016	Electronic	Business	Yes - Unknown #	Unknown

A copy of certain user account information was stolen from our systems in late 2014 by what we believe is a state-sponsored actor. We are closely coordinating with law enforcement on this matter and working diligently to protect you. The stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Yahoo
 Article URL: https://oag.ca.gov/system/files/Yahoo%20Notification%20Documents_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-03	UC San Diego School of Medicine	CA	9/15/2016	Electronic	Educational	Yes - Unknown #	Unknown

This letter is to inform you that on September 7, 2016, UC San Diego School of Medicine (UCSD SOM) became aware of an electronic file that was accessible on the internet containing the personal information of individuals.

Attribution 1 Publication: CA AG's office Author:
 Article Title: UC San Diego School of Medicine
 Article URL: https://oag.ca.gov/system/files/Final%20GME%20Notice%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-02	Stallcup & Associates, CPAs	CA	9/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 11th, our firm was subject to a ransomware virus wherein some of our network computer files were encrypted without our permission. If you are an individual, this information may have included your name, gender, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information, as well as direct deposit bank account information, including account number and routing information (if provided to us), and supporting records.

Attribution 1 Publication: CA AG's office / databreaches.net Author:
 Article Title: Stallcup & Associates, CPAs
 Article URL: https://oag.ca.gov/system/files/Stallcup%20Final%20Multi%20Letter%20Sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160923-01	USC Keck Medical Center	CA	8/1/2016	Electronic	Medical/Healthcare	Yes - Published #	16,000

On August 1st 2016, USC Keck and Norris Hospitals detected ransomware on two servers after being notified earlier that day that certain hospital employees could not access their files. Our investigation is continuing, but to date, we have identified the following categories of documents that had sensitive data and that were encrypted by the malware attack. Sensitive data included name and demographic information, date of birth, identifiable health information, including treatment and diagnosis for some patients, and in certain cases, social security numbers.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
 Article Title: USC Keck Medical Center
 Article URL: https://oag.ca.gov/system/files/NOTICE%20%5BFINAL%5D_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160922-03	Genghis Grills	TX	9/19/2016	Electronic	Business	Yes - Unknown #	Unknown

Four Dallas-area Genghis Grill restaurants experienced breaches in their payment processing systems starting as early as February, the company reported on its website Friday. The operator said hackers installed malware in the system to capture payment card information, including names, account numbers, expiration dates and verification codes. Genghis Grill said the malware has been disabled, and security upgrades have been implemented.

Attribution 1 Publication: Nation's Restaurant News Author:
 Article Title: Genghis Grill reports data breach
 Article URL: <http://nrrn.com/technology/genghis-grill-reports-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160922-02	KidsPeace	PA	9/20/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,456

A box containing confidential client health information disappeared from an office at KidsPeace's Schnecksville facility, but the agency says it believes the records were not "inappropriately" removed or accessed. It was unclear from a written statement released Tuesday whether the records — which include names, birth dates, medical record reference numbers, patient account numbers and service dates — may have been lost or accidentally destroyed.

Attribution 1 Publication: mcall.com / hhs.gov Author:
 Article Title: KidsPeace announces possible client information breach
 Article URL: <http://www.mcall.com/news/breaking/mc-kidspeace-records-breach-20160920-story.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160922-01	Ventura County Health Care Agency	CA	9/20/2016	Electronic	Government/Military	Yes - Published #	777

A July data breach involving names, birth dates and other information affected 777 patients, Ventura County Health Care Agency officials said Tuesday. A letter notifying affected patients in the county-run health system was sent on Sept. 13. Officials said the data breach happened on July 11 when an employee took home paperwork and apparently misplaced it. The material was recovered within the employee's home by an acquaintance who returned the material to the agency.

Attribution 1 Publication: vcstar.com / hhs.com Author:
Article Title: County health care agency reports breach of patient data
Article URL: <http://www.vcstar.com/story/news/local/2016/09/20/county-health-care-agency-reports-breach-patient-data/90750126/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-10	UIL Holdings Corporation	CT	9/16/2016	Electronic	Business	Yes - Published #	116

On August 4, 2016, in connection with a rate case proceeding before the Connecticut Public Utilities Regulatory Authority (PURA), UIL's subsidiary, The United Illuminating Company, filed a copy of a report that included an attachment that contained SPII, specifically, the names, social security numbers and 401(k) Plan account balances of 116 former employees of UIL or its affiliates, one of whom is a resident of New Hampshire.

Attribution 1 Publication: NH AG's office Author:
Article Title: UIL Holdings Corporation
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/uil-holdings-20160916.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-09	QR Lending	FL	9/2/2016	Electronic	Banking/Credit/Financial	Yes - Published #	1,487

On June 29, 2016, QR Lending discovered that phishing emails were sent from two of its employees' email addresses. QR Lending immediately launched an investigation and retained third party forensic experts to assist in the investigation of the incident. QR Lending determined that the unauthorized individual or individuals who used the two employee's email accounts to send the phishing emails had access to the email messages in those accounts. For affected individuals that reside in New Hampshire, the personal information contained in the email accounts was some combination of name, Social Security number, driver's license number, address, date of birth, bank account number and Tax Identification Number. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: QR Lending
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/qr-lending-20160902.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-08	Masy BioServices / Masy Systems, Inc.	MA	9/8/2016	Electronic	Business	Yes - Published #	145

On September 2, 2016, Masy learned that employee wage and tax information was inadvertently compromised as a result of an email phishing scheme. Masy immediately investigated this incident and determined that, on August 5, 2016, a Masy employee received a "spoofed" email requesting distribution of all employees' W-2 information. The sender of the email has not yet been identified but Masy has learned that the Internal Revenue Service (IRS) has reported a recent increase in similar incidents, where a hacker impersonates an authorized person in an attempt to obtain W-2 and other similar employee information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Masy BioServices / Masy Systems, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/masy-bioservices-20160908.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-07	FraserCPA	NJ	9/13/2016	Electronic	Business	Yes - Unknown #	Unknown

Yesterday, I contacted a CPA firm in New Jersey that had been hacked by a Russian hacker known as "Return" (among other aliases). During a chat, Return had told me that he had hacked FraserCPA and had obtained more than 12 GB of data – W-2 statements, tax returns, correspondence, etc. As proof, he sent me 500mb of files.

Attribution 1 Publication: databreaches.net Author:
Article Title: Maplewood tax firm hacked; data held for ransom
Article URL: <https://www.databreaches.net/nj-maplewood-tax-firm-hacked-data-held-for-ransom/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-06	Hickey Law Firm	FL	9/12/2016	Electronic	Business	Yes - Unknown #	Unknown

As DataBreaches.net learned, the same Russian hacker who hacked Man Alive clinic in Baltimore also hacked Hickey Law Firm in Florida. And as he did with Man Alive, he also issued a ransom demand: pay him 18 BTC by the end of this month or he will put all the data up for sale. In this case, he claims the data includes all of one of the lawyers' emails, client information including SSN and date of birth, as well as wire transfer instructions and more.

Attribution 1 Publication: databreaches.net / The Recorder Author:
Article Title: Law Firms Are "One-Stop Shopping" for Hackers, as Hickey Law Firm Found Out
Article URL: <https://www.databreaches.net/law-firms-are-one-stop-shopping-for-hackers-as-hickey-law-firm-found-out/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-05	Man Alive, Inc. / Lane Treatment Center	MD	9/8/2016	Electronic	Business	Yes - Unknown #	Unknown

The non-profit organization Man Alive in Baltimore provides substance abuse treatment and mental health services to some of the city's neediest residents. As if the facility didn't have enough challenges, on August 24, they were hacked, and a patient database with sensitive personal and treatment information was put up for sale on the dark web.

Attribution 1 Publication: databreaches.net Author:
Article Title: Baltimore addiction treatment clinic hacked; patients' info up for sale on dark web
Article URL: <https://www.databreaches.net/baltimore-addiction-treatment-clinic-hacked-patients-info-up-for-sale-on-dark-web/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-04	ClixSense	NC	9/13/2016	Electronic	Business	Yes - Unknown #	Unknown

Troy Hunt, operator of the breach notification service Have I Been Pwned?, said he reviewed the file and concluded it almost certainly contains data taken from ClixSense. Besides unhashed passwords and e-mail addresses, the dump includes users' dates of birth, sex, first and last names, home addresses, IP addresses, account balances, and payment histories.

Attribution 1 Publication: databreaches.net Author:
Article Title: 6.6 million plaintext passwords exposed as site gets hacked to the bone
Article URL: <http://arstechnica.com/security/2016/09/plaintext-passwords-and-wealth-of-other-data-for-6-6-million-people-go-public/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-03	Oconee County	SC	9/16/2016	Electronic	Government/Military	Yes - Published #	230

230 Oconee County employees did not get money deposited into their bank accounts after a data breach involving the payroll service the county uses. The Sheriff's Office says they do not have an exact dollar amount from the breach but they are working with SLED and the FBI to investigate.

Attribution 1 Publication: databreaches.net / WSPA.com Author:
Article Title: Data breach in Oconee Co. causes employee pay issues
Article URL: <http://wspa.com/2016/09/16/some-employees-not-paid-after-data-breach-in-oconee-co/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-02	La Joya American Federation of Teachers	TX	9/17/2016	Electronic	Educational	Yes - Unknown #	Unknown

La Joya police chief Raul Gonzalez tells CHANNEL FIVE NEWS a representative who works at La Joya American Federation of Teachers accidentally sent out an email. That email contained the social security numbers and payroll deductions of 1600 La Joya ISD teachers. The school district started deleting the emails that were accidentally released

Attribution 1 Publication: databreaches.net / KRGV.com Author:
Article Title: Personal Information of La Joya ISD Teachers Accidentally Released
Article URL: <http://www.krgv.com/story/33121425/personal-information-of-la-joya-isd-teachers-accidentally-released>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160920-01	Saint Francis Health System	OK	9/19/2016	Electronic	Medical/Healthcare	Yes - Published #	6,000

Saint Francis Health System said in a statement it was notified by email on September 7, 2016, about an unauthorized external access of a server, and patient information was obtained. Roberts said after working with forensics investigators, they discovered the information taken from the server appears to be a list of about 6,000 names and addresses. She said Social Security numbers, driver's license and financial information are not included on the list.

Attribution 1 Publication: [databreaches.net / newson6.com](http://databreaches.net/newson6.com) Author:
Article Title: Saint Francis Investigating Security Breach
Article URL: <http://www.newson6.com/story/33131054/saint-francis-investigating-security-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-17	Decatur Health Systems	KS	9/9/2016	Paper Data	Medical/Healthcare	Yes - Published #	707

Oberlin, KS-based Decatur Health Systems (DHS) has started notifying 707 patients about the potential theft of a limited amount of their protected health information. The PHI was recorded in a binder that was being used by a radiology technician to monitor X-ray doses. No Social Security numbers were recorded, although the binder contained names, dates of birth, the reason for performing CAT scans, test dates, X-ray doses, and the names of referring physicians.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: DECATUR HEALTH SYSTEMS INFORM 707 PATIENTS OF POTENTIAL PHI THEFT
Article URL: <http://www.hipaajournal.com/decatour-health-systems-707-patients-potential-phi-theft-3586/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-16	King of Prussia Dental Associates	PA	9/12/2016	Electronic	Medical/Healthcare	Yes - Published #	16,228

King of Prussia Dental Associates (KOPDA) has announced that a third party may have gained access to a server containing the protected health information of its patients. Data stored on the server included names, dates of birth, Social Security numbers, phone numbers, addresses, details of treatment provided to patients, and patient account numbers.

Attribution 1 Publication: [hipaajournal.com / NH AG's office / hhs](http://hipaajournal.com/NH%20AG's%20office/hhs) Author:
Article Title: KING OF PRUSSIA DENTAL ASSOCIATES ANNOUNCES POTENTIAL PHI BREACH
Article URL: <http://www.hipaajournal.com/king-of-prussia-dental-associates-announces-potential-phi-breach-3589/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-15	Signature Financial	PA	9/13/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On or about July 27, 2016, we discovered that an unknown individual or individuals may have gained access to the personal email account of an employee of Signature Financial. This email account contained, among other things, personally identifiable information of certain Signature Financial clients and employees. We immediately took steps to secure the email account and launched an investigation to determine whether any sensitive information was accessed or acquired.

Attribution 1 Publication: VT AG's office Author:
Article Title: Signature Financial
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Signature%20Financial%20LLC%20SBN%20to%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-13	Ursus Holdings	TX	9/15/2016	Electronic	Business	Yes - Unknown #	Unknown

We first detected suspicious email account activity on April 25, 2016, when an employee's email account began sending "blast" or "spam" emails. That employee previously had received a phishing email requesting account credentials to access what appeared to be a secure PDF attachment. Upon the employee providing the credentials, others within the employee's contact list began receiving similar emails. Three other employees are believed to have received the same email attachment and provided their credentials.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Ursus Holdings
Article URL: https://oag.ca.gov/system/files/California%20Notification%20Proof_1.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 87 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-12	Menzies Aviation, Inc. 401(k) plan / Ascensus, Inc.	PA	9/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 23, 2016, we discovered a website configuration error that allowed the plan administrator of another Ascensus retirement plan access to your personal information. Upon discovering this, Ascensus immediately terminated the configuration that allowed this inadvertent access.

Attribution 1 Publication: CA AG's office Author:
Article Title: Menzies Aviation, Inc. 401(k) plan / Ascensus, Inc.
Article URL: https://oag.ca.gov/system/files/211253%20MENZIES%20AVIATION%20-%20%20PPT%20Letter%20-%20General_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-11	Rebecca Minkoff	NY	9/9/2016	Electronic	Business	Yes - Published #	6,855

On August 10, 2016, Rebecca Minkoff learned that there may have been unauthorized access to our website. We hired an outside forensic expert to determine whether the incident resulted in the unauthorized access to any personal information. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / VT AG' Author:
Article Title: Rebecca Minkoff
Article URL: https://oag.ca.gov/system/files/Pages%20from%20REV3_EXPERIAN_C2679_NOTICE_LETTER_TO_CONSUMERS_%28

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-10	M Holdings Securities	OR	7/29/2016	Electronic	Banking/Credit/Financial	Yes - Published #	19,012

Portland-based M Holdings Securities Inc., a subsidiary of M Financial Holdings Inc., has informed California's attorney general of a stolen laptop with client information, including social security numbers. (Consumers affected per IN AG's office)

Attribution 1 Publication: Portland Business Journal / CA AG's Off Author:
Article Title: One of Portland's largest financial firms warns of possible data breach
Article URL: <http://www.bizjournals.com/portland/news/2016/09/12/one-of-portlands-largest-financial-firms-warns-of.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-09	Office of Pratap S. Kurra, M.D.	CA	8/8/2016	Paper Data	Medical/Healthcare	Yes - Published #	2,029

On August 9, 2016, I was informed that papers related to my practice were found in a trash container. I immediately began an investigation into the matter and determined that on August 8, 2016, the day before, billing tickets used by my practice were accidentally thrown away during my move. Fortunately, all known records were retrieved within 24 hours, and upon further investigation, it was determined to have been a singular incident.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Office of Pratap S. Kurra, M.D.
Article URL: https://oag.ca.gov/system/files/Pratap%20Kurra%20MD_Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-08	Lulu's Fashion Lounge	CA	8/16/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 23, 2016, we discovered that our payment card processing system may have been accessed without our authorization. We immediately launched a full investigation, including working with a third-party digital forensic investigator. We determined that the unauthorized access occurred intermittently between August 11 and August 16, 2016, and only affected customers entering a payment card new to our system.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Lulu's Fashion Lounge
Article URL: https://oag.ca.gov/system/files/Lulus%20Consumer%20Notice_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-07	St. Elizabeth Physicians (Summit Medical Group)	KY	8/23/2016	Electronic	Medical/Healthcare	Yes - Published #	674

On July 12, 2016 St. Elizabeth Physicians inadvertently released the email addresses of 674 individuals in an email sent by its Weight Management Center inviting the recipients to a vitamin presentation and open forum meeting. The sender inadvertently and mistakenly failed to blind copy the recipients thus allowing all email addresses to be visible by all recipients. No social security numbers, phone numbers, addresses, or any other personal health or identification information was disclosed. The only information disclosed was email addresses.

Attribution 1 Publication: [databreaches.net / hhs.gov](http://databreaches.net/hhs.gov) Author:
Article Title: St. Elizabeth Physicians' email gaffe exposed patient email addresses
Article URL: <https://www.databreaches.net/st-elizabeth-physicians-email-gaffe-exposed-patient-email-addresses/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-06	CalOptima #1	CA	8/22/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,000

On October 7, 2015, an internal printing error resulted in approximately 100 CalOptima Medi-Cal members with diabetes receiving a health incentive survey that may have included an extra survey meant for another member. We became aware of the error on October 8, 2015, and immediately stopped all printing. However, we were not able to retrieve the surveys that had already been processed for mailing. (Note: number of exposed records per HHS.gov)

Attribution 1 Publication: [hhs.gov / company website / databreach](http://hhs.gov/company-website/databreach) Author:
Article Title: CalOptima notifies members of breach 8 months later?
Article URL: <https://www.databreaches.net/caloptima-notifies-members-of-breach-8-months-later/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-05	Los Angeles County Department of Health	CA	8/30/2016	Paper Data	Government/Military	Yes - Published #	743

Los Angeles County Department of Health Services officials said appointment lists containing 743 patients' personal information were stolen in the breach after a hospital employee discovered their car had been broken into on July 8, according to NBC 4 news. Information in the appointment lists included full names, birth dates, medical record numbers, phone numbers, genders, clinics and appointment information.

Attribution 1 Publication: [hhs.gov / beckershospitalreview.com](http://hhs.gov/beckershospitalreview.com) Author:
Article Title: 743 patients' information compromised in vehicle break-in at California hospital
Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/743-patients-information-compromised-in-v>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-04	Geisinger Health Plan	PA	9/7/2016	Electronic	Medical/Healthcare	Yes - Published #	2,814

Danville, Pa.-based Geisinger Health Plan is notifying members of a data breach after a processing error resulted in invoices being mailed to incorrect recipients. Information contained in the invoices includes members' names, birth dates, health insurance premium information, member identification number and smoking status. No medical treatment or financial information was included in the statements.

Attribution 1 Publication: [hhs.gov / Becker's Hospital Review](http://hhs.gov/Becker's-Hospital-Review) Author:
Article Title: Geisinger Health Plan
Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/geisinger-health-plan-mailing-error-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-03	University Gastroenterology, Inc.	RI	9/8/2016	Electronic	Medical/Healthcare	Yes - Published #	15,478

Providence, R.I.-based specialty group University Gastroenterology is warning patients of a cyberattack the organization became aware of in July. "We determined that some files may have contained patient names, addresses, dates of birth, Social Security numbers, and medical billing information," the notification reads. "Patients' electronic medical records were not exposed and remain secure."

Attribution 1 Publication: [hhs.gov / beckershospitalreview.com / N](http://hhs.gov/beckershospitalreview.com/N) Author:
Article Title: RI gastroenterology center alerts patients to possible breach after finding encrypted files
Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/ri-gastroenterology-center-alerts-patients-t>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 89 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-02	U.S. Healthworks	CA	9/9/2016	Electronic	Medical/Healthcare	Yes - Published #	1,400

A laptop computer containing the PHI of 1,400 patients was recently stolen from a U.S. HealthWorks employee. While this would not usually result in the issuing of breach notifications to patients, in this case the employee had written down the password to access the device and decrypt data. The password was kept with the laptop and it was also stolen.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](http://hhs.gov/hipaajournal.com) Author:
Article Title: U.S. HEALTHWORKS ANNOUNCES THEFT OF ENCRYPTED LAPTOP AND DECRYPTION KEY
Article URL: <http://www.hipaajournal.com/u-s-healthworks-announces-theft-encrypted-laptop-decryption-key-3591/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160919-01	CHI Franciscan Health / St. Clare Hospital / St. Joseph	WA	9/16/2016	Electronic	Medical/Healthcare	Yes - Published #	2,818

CHI Franciscan Health St. Clare Hospital and St. Joseph Medical Center WA Healthcare Provider 2818 09/16/2016 Unauthorized Access/Disclosure Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: CHI Franciscan Health / St. Clare Hospital / St. Joseph Medical Center
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160915-03	Office of Michelle A. Pecora CPA	OR	8/25/2016	Electronic	Business	Yes - Unknown #	Unknown

Ms Resora determined that between July 27,2016 and August 2,2016, her office was broken into and a laptop was stolen. The laptop contained personally identifiable information pertaining Ms. Pecora's clients.

Attribution 1 Publication: OR AG's office / MT AG's office Author:
Article Title: Office of Michelle A. Pecora CPA
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/261051790>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160915-02	Wheeler & Egger	CA	8/9/2016	Electronic	Business	Yes - Unknown #	Unknown

As reported to you in our communication of August 22, on August 15, 2016, we discovered a data security incident involving our firm and your personal information. Our tax software company reported to us that the IRS reported to them that your tax return had been e-filed. Knowing that we had not filed the return and conferring with both our software company and the IRS, it became evident that someone, other than you or us, had filed your return and a total of 44 other clients, on dates between August 3rd and August 9th, 2016.

Attribution 1 Publication: CA AG's office / databreaches.net / SC Author:
Article Title: Wheeler & Egger
Article URL: https://oag.ca.gov/system/files/Wheeler%20Letter%201s_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160915-01	Yuba Sutter Medical Clinic	CA	9/11/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On or about August 3, 2016, the Yuba-Sutter Medical Clinic's computer system came under a "ransomware attack" by hackers. Ransomware attacks are designed to deny access to certain portions of a computer system until a ransom is paid.

Attribution 1 Publication: CA AG's office Author:
Article Title: Yuba Sutter Medical Clinic
Article URL: https://oag.ca.gov/system/files/2016_09_11_21_53_08_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 90 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160908-08	Merrimack Mortgage	NH	9/2/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On August 3th, 2016, three (3) of our employee email accounts were compromised due to a phishing attack on our organization. The phishing attack consisted of a message appearing to come from a legitimate person with a link to click on which would take them to a document. The link brought them to a form to fill out to retrieve the document and the form was used to collect our employee's login information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Merrimack Mortgage
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/merrimack-mortgage-20160902.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160908-07	Exterran	TX	8/25/2016	Electronic	Business	Yes - Published #	10,844

On November 24, 2015, an Exterran Human Resources employee had an Exterran-issued laptop stolen from the employee's car. The theft occurred in Houston, Texas, and the employee reported it to Exterran and local law enforcement. The laptop was password-protected. The laptop also contained a feature that would allow all information stored on the laptop to be remotely "wiped" or deleted if an attempt were made to access the Internet through the laptop. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH Ag's office / IN AG's office Author:
Article Title: Exterran
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/externan-20160825.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160908-06	Jerry's Artarama N.C., Inc.	NC	7/10/2016	Electronic	Business	Yes - Unknown #	Unknown

Although we had taken measures that we believe were commercially reasonable under the circumstances, we may have been subject to a sophisticated cyber-attack that appears to have potentially penetrated our defenses. Malicious code may have been placed on our system and based upon our investigation, appears to have intercepted customer information that was transmitted during purchase transactions from May 3rd, 2016 until July 10th, 2016.

Attribution 1 Publication: CA AG's office / OR AG's office Author:
Article Title: Jerry's Artarama N.C., Inc.
Article URL: <https://oag.ca.gov/system/files/Form%20of%20Customer%20Notice%20Letter%20re%20Breach%20-%20Jerrys%20Arta>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160908-05	Southwest Portland Dental / Patterson Dental Supply, Inc.	OR	9/2/2016	Electronic	Medical/Healthcare	Yes - Published #	1,980

Patterson Dental Supply Inc. (PDSI) is a trusted third-party vendor that provides software to dentists to help manage dental practice information. On July 1, 2016, we determined that between April 2012 and January 2016 one or more unauthorized individuals gained access to a network resource site used by SPD and PDSI in 2010 to exchange data between software systems.

Attribution 1 Publication: OR AG's office / hhs.gov Author:
Article Title: Southwest Portland Dental / Patterson Dental Supply, Inc.
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1841081963>

Attribution 2 Publication: databreaches.net / OR AG's office Author:
Article Title: Southwest Portland Dental notifies patients of Patterson Dental breach
Article URL: <https://www.databreaches.net/southwest-portland-dental-notifies-patients-of-patterson-dental-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160908-04	Nourse Farms	MA	8/31/2016	Electronic	Business	Yes - Published #	6,320

We recently Identified a security issue that affected our ecommerce site between February 22, 2016 and July 16, 2016, and resulted in an unauthorized access of customer information by a third party. Our website, noursefarms.com was one of over 300 online ecommerce sites to be invaded by a hack that targeted a specific software platform. Once discovered, we took immediate steps to stop the breach and prevent future breaches.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: Nourse Farms
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/nourse-farms-20160831.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160908-03	U.S. Customs and Border Protection	DC	9/6/2016	Electronic	Government/Military	Yes - Published #	5,000

Customs and Border Protection released the personally identifiable information, including Social Security numbers, of thousands of individuals to dozens of federal agencies during an investigation of cheating on polygraph tests. CBP violated some aspects of the Privacy Act in distributing the information across government, the Homeland Security Department's inspector general found in its report. The agency collected and distributed information such as Social Security numbers, email and mailing addresses, and phone numbers of individuals who had purchased materials from two individuals who helped job applicants pass polygraphs.

Attribution 1 Publication: Government Executive Author:
Article Title: DHS Exposes Thousands of Individuals' Private Information -- Including Feds, Golfers and Priests
Article URL: <http://www.govexec.com/oversight/2016/09/dhs-exposes-thousands-individuals-private-information-including-feds-gol>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160908-02	Children's Mercy Hospital	MO	9/5/2016	Paper Data	Medical/Healthcare	Yes - Published #	238

Children's Mercy Hospital in Kansas City, MO has announced that 238 children's medical records have been stolen from a vehicle used by a hospital employee. The vehicle was locked and the records were stored in a hard-sided case, which was also locked. However, it is probable that the thieves managed to open the case and view the contents.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Children's Mercy Hospital Announces Breach of Children's PHI
Article URL: <http://www.hipaajournal.com/childrens-mercy-hospital-announces-breach-of-childrens-phi-3579/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160908-01	Burrell Behavioral Health	MO	9/5/2016	Electronic	Medical/Healthcare	Yes - Published #	7,748

Springfield Missouri-based Burrell Behavioral Health has announced it has been the subject of a cyberattack which has potentially resulted in the protected health information of certain patients being obtained by unauthorized individuals.

Attribution 1 Publication: hipaajournal.com / kspr.com Author:
Article Title: Patients Notified of Burrell Behavioral Health Cyberattack and PHI Exposure
Article URL: <http://www.hipaajournal.com/patients-notified-burrell-behavioral-health-cyberattack-phi-exposure-3580/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160907-08	University of Alaska Mat-Su Campus	AK	9/7/2016	Electronic	Educational	Yes - Published #	5,416

On Tuesday, University of Alaska officials announced an attacker using employee credentials may have accessed student information. How many victims? Approximately 5,416. What type of information? Names, social security numbers, transcripts, appeals forms, grant award amounts, addresses, and phone numbers where potentially compromised in the breach.

Attribution 1 Publication: scmagazine.com Author:
Article Title: University of Alaska breach may have exposed student info
Article URL: <http://www.scmagazine.com/university-of-alaska-breach-may-have-exposed-student-info/article/520975/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160907-07	Stand Up Desk Store (SUDS)	AL	8/31/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently became aware of a malware intrusion affecting our e-commerce platform by targeting customers' payment card information. Promptly after discovering the intrusion, we contained it and conducted an in-depth investigation, engaging outside cybersecurity experts to determine the facts. We estimate that the malware operated between July 3 and July 22, 2016. Based on our investigation, we believe this unauthorized person may have accessed documents or records containing your name, billing address, email address and credit card number (including CCV number).

Attribution 1 Publication: VT AG's office Author:
Article Title: Stand Up Desk Store (SUDS)
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/SUDS%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160907-06	Vulcan Industries	AL	8/31/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently became aware of a malware intrusion affecting our Siegel Display Products e-commerce platform by targeting customers' payment card information. Promptly after discovering the intrusion, we contained it and conducted an in-depth investigation, engaging outside cybersecurity experts to determine the facts. We estimate that the malware operated between July 3 and July 22, 2016. Based on our investigation, we believe this unauthorized person may have accessed documents or records containing your name, billing address, email address and credit card number (including CCV number).

Attribution 1 Publication: VT AG's office Author:
Article Title: Vulcan Industries
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Vulcan%20Industriues%20SBN%20to%20Consumers.p

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160907-05	Village of Oak Park	IL	8/18/2016	Electronic	Medical/Healthcare	Yes - Published #	688

The breach in question dates back to January. On January 22, 2016, officials at Village of Oak Park discovered an employee had emailed spreadsheets containing the PHI of 688 individuals to a personal email account.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Another Employee is Fired for Emailing PHI to a Personal Account
Article URL: <http://www.hipaajournal.com/another-employee-is-fired-for-emailing-phi-to-a-personal-account-3581/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160907-04	Planned Parenthood of Greater Washington and	WA	8/26/2016	Electronic	Medical/Healthcare	Yes - Published #	10,700

An email incident has been reported to the Department of Health and Human Services' Office for Civil Rights that has impacted 10,700 individuals. On June 28, 2016, Planned Parenthood of Greater Washington and North Idaho discovered that emails had been accidentally sent to incorrect recipients.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Planned Parenthood of Greater Washington and North Idaho Informs Patients of Email Incident
Article URL: <http://www.hipaajournal.com/medstar-health-cardiology-associates-terminates-employee-for-phi-theft-3578/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160907-03	New York State Psychiatric Institute	NY	8/15/2016	Electronic	Business	Yes - Published #	21,880

New York State Psychiatric Institute has reported that unauthorized individuals have gained access to parts of the institute's computer system which was used to store the protected health information of 21,880 research participants. The intrusion was detected on June 17, 2016, although the subsequent investigation revealed that the system was accessed by unauthorized individuals between April 28 and May 4, 2016.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: New York State Psychiatric Institute
Article URL: <http://www.hipaajournal.com/new-york-state-psychiatric-institute-reports-22k-record-phi-breach-3574/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160907-02	CHI Franciscan Healthcare Highline Medical Center / R-C	WA	9/1/2016	Electronic	Medical/Healthcare	Yes - Published #	18,399

On July 22, 2016, R-C Healthcare Management, a vendor working on behalf of Highline Medical Center advised Highline that files containing patient information had inadvertently been left accessible via the internet by R-C Healthcare, from April 21, 2016 to June 13, 2016. R-C Healthcare performed services for Highline Medical Center prior to CHI's acquisition of Highline Medical Center in 2014. The data involved was used in cost reporting functions from years 1993-1994 and 2008 – 2013.

Attribution 1 Publication: hhs.gov / VT AG's office / databreaches. Author:
Article Title: CHI Franciscan Healthcare Highline Medical Center
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/CHI%20Franciscan%20Healthcare%20Highline%20Med

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160907-01	Cardiology Associates	MD	8/10/2016	Electronic	Medical/Healthcare	Yes - Published #	907

An employee of Medstar Health's Cardiology Associates has been terminated after emailing the protected health information of 907 patients to a personal email account. The list contained the names of patients, their dates of birth, and health insurance ID numbers. Some Social Security numbers were also detailed on the list.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: MedStar Health Cardiology Associates Terminates Employee for PHI Theft
Article URL: <http://www.hipaajournal.com/medstar-health-cardiology-associates-terminates-employee-for-phi-theft-3578/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160906-03	Hutton Hotel	TN	9/5/2016	Electronic	Business	Yes - Unknown #	Unknown

The Hutton Hotel is warning customers about a data breach that may have compromised the credit card information of thousands of guests. The Hotel is working with police to determine how malware was installed to capture information on its payment processing system. Hutton Hotel says the breach included names, credit card numbers, verification codes and expiration dates for customers between September 2012 through April of 2015.

Attribution 1 Publication: fox17.com / databreaches.net / CA AG's Author:
Article Title: Hutton Hotel enhances security measures after breach
Article URL: <http://fox17.com/news/local/hutton-hotel-enhances-security-measures-after-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160906-02	Medical College of Wisconsin	WI	9/6/2016	Electronic	Medical/Healthcare	Yes - Published #	3,179

On July 5, the college noticed unusual activity associated with an employee's email account, according to a news release. Upon discovering the issue, MCW took action to prevent further access and began an investigation. The college retained an independent computer forensic firm to investigate the abnormal activity.

Attribution 1 Publication: wauwatosanow.com / hhs.gov Author:
Article Title: Medical College discloses security breach information
Article URL: <http://www.wauwatosanow.com/story/news/2016/09/06/medical-college-wisconsin-discloses-information-security-brea>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160906-01	Dropbox	CA	8/29/2016	Electronic	Business	Yes - Unknown #	Unknown

Data from a 2012 breach has resurfaced, leading to fears that the information could be used to compromise accounts. IT managers using a new Dropbox feature don't need to worry, but they still have to guard against employees' bad password hygiene. Among the half billion Dropbox users, those who have not changed their passwords since mid-2012 may wish to come up with another sequence of impossible-to-remember alphanumeric characters to authenticate themselves.

Attribution 1 Publication: informationweek.com Author:
Article Title: Dropbox Urges Users To Change Old Passwords
Article URL: <http://www.informationweek.com/devops/project-management/dropbox-urges-users-to-change-old-passwords/d/d-id/1>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160830-09	W.C. Ralston Architects	VA	8/16/2016	Electronic	Business	Yes - Unknown #	Unknown

RSI has advised our client that during the window of July 18 to July 25, 2016, a third party might have gained access to certain personal information of twenty nine (29) current and former employees, limited to name, address, telephone number, social security number and date of birth.

Attribution 1 Publication: NH Ag's office Author:
Article Title: W.C. Ralston Architects
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/w-c-ralston-architects-20160816.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160830-08	J. Polep Distribution Services	MA	8/17/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 29, 2016, J. Polep discovered that they were the victim of an email spoofing scam that resulted in the compromise of 2015 W -2 forms. Through this spoofing scam, a request was made from what appeared to be a legitimate J. Polep company, Consumer Products Distributors ("CPO"), email address for 2015 W-2 information. An employee W-2 includes the following categories of information: (1) the employee's name, and the employee's Social Security number.

Attribution 1 Publication: NH Ag's office Author:
Article Title: J. Polep Distribution Services
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/j-polep-distribution-20160817.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160830-07	Dennis Group	MA	8/12/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 5, 2016, Dennis Group discovered that its company was targeted in an email spoofing attack. Through this attack, a request was made for 2015 IRS Tax Form W-2 information. A report with some information, including names, addresses, Social Security numbers, and compensation information, was emailed before it was discovered that the request was made from a fraudulent account by an individual purporting to be Dennis Group's CEO.

Attribution 1 Publication: NH AG's office Author:
Article Title: Dennis Group
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/dennis-group-20160812.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160830-06	Birch Communications	CA	8/25/2016	Electronic	Business	Yes - Published #	1,913

Please be advised that on August 4, 2016, Birch Communications ("Company") learned that it experienced a data incident on that same date when one of its employees, while responding by email to an inquiry from a former employee, inadvertently attached a file containing personal information (including names and social security numbers) pertaining to certain current and other former employees

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: Birch Communications
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/birch-communications20160825.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160830-05	Millenium Hotels & Resorts	CO	8/25/2016	Electronic	Business	Yes - Unknown #	Unknown

Millennium Hotels & Resorts North America (MHR) has become aware of a data security incident involving food and beverage point of sale systems at 14 of its hotels in the United States.

Attribution 1 Publication: databreaches.net Author:
Article Title: Millennium Hotels & Resorts North America Informed of Potential Data Security Incident
Article URL: <https://www.databreaches.net/millennium-hotels-resorts-north-america-informed-of-potential-data-security-incident/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160830-04	Office of Dr. Richard Boehm	TN	8/25/2016	Paper Data	Medical/Healthcare	Yes - Published #	500

As required by law, this notice is to inform our patients that some of your confidential personal information may have been compromised. It has come to our attention that an employee may have printed documents containing some of our patients' personal information from our computer files and removed these documents from our office.

Attribution 1 Publication: databreaches.net Author:
Article Title: Tennessee dentist notifies patients of possible data theft by employee
Article URL: <https://www.databreaches.net/tennessee-dentist-notifies-patients-of-possible-data-theft-by-employee/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160830-03	Langston Hughes Young Explorers Academy	NY	8/26/2016	Paper Data	Educational	Yes - Unknown #	Unknown

In a shocking breach of confidential information, names, addresses, even social security numbers for students and parents were found outside a Bronx school. Eyewitness News has learned exclusively that the pile of papers contain extremely personal documents, including private medical information and social security numbers of students, documents that no one outside the school is supposed to see, but that were left fully exposed on the street for anyone to see.

Attribution 1 Publication: databreaches.net / WABC=TV Author:
Article Title: NYC students' personal info left on street in careless breach
Article URL: <https://www.databreaches.net/nyc-students-personal-info-left-on-street-in-careless-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160830-02	Appalachian Regional Healthcare	NC	8/30/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On Saturday August 27, 2016, a computer virus was discovered to have been installed on Appalachian Regional Healthcare's system. Computer systems were immediately shut down to prevent the spread of the virus to other systems. As a result, web based services and electronic communications have been affected.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: APPALACHIAN REGIONAL HEALTHCARE EXPERIENCES CYBERATTACK
Article URL: <http://www.hipaajournal.com/appalachian-regional-healthcare-experiences-cyberattack-3572/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160830-01	USC Medical Center	CA	8/30/2016	Paper Data	Medical/Healthcare	Yes - Published #	700

More than 700 patients of the neurosurgery clinic of LA County's USC Medical Center have been informed that some of their protected health information has been obtained by criminals. Printed lists of patients who had visited the LAC+USC neurosurgery clinic were stolen from the vehicle of an employee. The lists contained full names, genders, telephone numbers, medical record numbers, dates of birth, appointment times, reasons for appointments, and medical diagnoses.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: PHI BREACH REPORTED BY LA COUNTY USC MEDICAL CENTER
Article URL: <http://www.hipaajournal.com/phi-breach-reported-by-la-county-usc-medical-center-3573/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160829-07	Arizona Department of Administration	AZ	8/29/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

According to Matthew Roberts, Director of Communications for the Arizona Secretary of State, in late May, Arizona officials took the statewide voting registration system offline after the FBI alerted the Arizona Department of Administration that there was a credible cyber threat to the voter registration system.

Attribution 1 Publication: cnn.com Author:
Article Title: Officials: Hackers breach election systems in Illinois, Arizona
Article URL: <http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160829-06	Illinois Board of Elections	IL	8/29/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

In Illinois, hackers accessed a database for the Illinois Board of Elections, compromising up to 200,000 personal voter records according to Ken Menzel, General Counsel for the board. The Illinois database included voters' names, addresses, sex and birthdays in addition to other information. Some of the records include either last four digits of a voter's social security number or drivers' license numbers.

Attribution 1 Publication: [cnn.com](#) Author:
Article Title: Officials: Hackers breach election systems in Illinois, Arizona
Article URL: <http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160829-05	Phoenix Dental Care	TN	8/15/2016	Paper Data	Medical/Healthcare	Yes - Published #	6,441

Phoenix Dental Care TN Healthcare Provider 500 08/15/2016 Theft Paper/Films

Attribution 1 Publication: [hhs.gov](#) Author:
Article Title: Phoenix Dental Care
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160829-04	Liberty Mountain Sports, LLC	UT	8/26/2016	Electronic	Business	Yes - Unknown #	Unknown

Liberty Mountain was the victim of an email "phishing" scam that caused Liberty Mountain inadvertently to disclose confidential information of approximately 300 employees in 3 states. If you are receiving this notice, your name, social security number, 2015 wages, date of birth, and address were inadvertently disclosed to an unknown party.

Attribution 1 Publication: VT AG's office Author:
Article Title: Liberty Mountain
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Liberty%20Mountain%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160829-03	Noble House Hotels & Resorts - Ocean Key Resort &	WA	8/24/2016	Electronic	Business	Yes - Unknown #	Unknown

Noble House was notified by the Secret Service on July 13, 2016, about possible fraudulent activity on the payment card system for one of its properties, Ocean Key Resort & Spa. We promptly began an investigation and engaged a computer security firm to examine our payment system for any signs of an issue. On July 26, 2016, the computer security firm confirmed that Ocean Key's system may have been compromised between April 26, 2016 and June 8, 2016.

Attribution 1 Publication: VT AG's office / CA AG's office Author:
Article Title: Noble House Hotels & Resorts - Multiple properties
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Ocean%20Key%20Resort%20and%20Spa%20SBN%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160829-02	Toyota Motor Credit Corporation	CA	6/28/2016	Electronic	Business	Yes - Published #	8,989

On June 28, 2016, a TFS associate mistakenly emailed a spreadsheet containing customer information to her personal email account. The email was sent using an encrypted transmission method. This incident was discovered on June 28, 2016. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / IN AG' Author:
Article Title: Toyota Motor Credit Corporation
Article URL: https://oag.ca.gov/system/files/2008%20--%20CUSTOMER%20Letter%20for%20AG_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160829-01	Sacramento County	CA	8/8/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

An error was discovered in the online automated application system within the Accela software that may have made your personal data available to Emergency Medical Service license applicants that had an account on the system. What Information Was Involved? Your name, address, social security number, driver's license, phone number, and date of birth.

Attribution 1 Publication: CA AG's office Author:
Article Title: Sacramento County
Article URL: https://oag.ca.gov/system/files/Updated%20Sac%20Co%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160825-04	Burke Mountain	VT	8/24/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to you because of the security breach you were first alerted to on July 12, 2016. You received the notification because your purchase of a season pass fell between the periods of 6am Sunday, July 10th through 6:30pm Monday, July 11th. This was the time in which your credit card information may have been compromised. This letter is meant as a reminder to you to take steps to protect yourself but should not be taken as an indication of any new threat related to this very specific incident.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Burke Mountain
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Burke%20Mountain%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160825-03	DXE Medical	TN	8/18/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On July 28, 2016, we were advised by our third-party website developer that it had identified code it did not recognize on the server that operates our e-commerce website. We immediately began an investigation, removed the code, and determined that the code was designed to copy data that was entered by customers during the checkout process.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
 Article Title: DXE Medical
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/DXE%20Medical%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160825-02	Precision Pipeline, LLC	WI	8/15/2016	Electronic	Business	Yes - Published #	3,675

On July 25, 2016, an e-mail phishing attack directed at Precision resulted in the disclosure of your first and last name, Social Security number ("SSN") and annualized compensation and tax withholding information. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / IN AG's Author:
 Article Title: Precision Pipeline, LLC
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Precision%20Pipeline%20SBN%20to%20Consumers.p

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160825-01	Penn State Alumni Association / ComNet	PA	8/15/2016	Electronic	Business	Yes - Unknown #	Unknown

The Penn State Alumni Association (PSAA) recently learned that one of its contractors, ComNet Marketing Group, Inc. (ComNet), experienced a security breach of the computer server that stored PSAA members' credit card information. ComNet's computer server deletion occurred around April 24, 2016. Upon learning of the incident, ComNet launched a forensic investigation and determined that an unauthorized user had gained administrative access and issued commands to delete files containing PSAA members' personal information from its computer server.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Penn State Alumni Association / ComNet Marketing Group)
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Penn%20State%20Alumni%20Assoc%20SBN%20to%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-16	Orleans Medical Clinic	IN	8/24/2016	Electronic	Medical/Healthcare	Yes - Published #	6,890

On or about April 17, 2016, we became aware of suspicious activity involving one of our computer servers. We initiated an investigation and learned that our computer server that contained electronic health record data had been left unsecured after the server was upgraded. As a result, computer hackers gained access to the server over a period of time from April 5, 2016 until April 17, 2016. On July 21, 2016, we received confirmation of the individuals and information potentially affected by the breach.

Attribution 1 Publication: databreaches.net / IN AG's office / hhs.g Author:
 Article Title: Orleans Medical Clinic Patient Information Breach
 Article URL: <https://www.databreaches.net/in-orleans-medical-clinic-patient-information-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-15	SocialBlade	US	8/16/2016	Electronic	Business	Yes - Unknown #	Unknown

The hack reportedly occurred in August 2016, and the hackers gained access to 273,086 users' details and 13,009 forum accounts. The leaked account data includes users' email address, IP address, username, user identifier and password.

Attribution 1 Publication: Author:
Article Title: SocialBlade Suffers Breach, User Data Leaked
Article URL: <http://www.batblue.com/socialblade-suffers-breach-user-data-leaked/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-14	Center for Neurosurgical and Spinal Disorders	LA	8/17/2016	Electronic	Medical/Healthcare	Yes - Published #	1,134

On the morning of July 21, 2016, we detected an unauthorized intruder in one of our computers. Access to this computer was immediately shut down; subsequently, CNSD's servers and network were taken offline. CNSD's IT professional, who after performing an investigation, determined that a hacker had gained remote access to the office manager's computer and installed both a program which recorded the user's keystrokes, and a program that periodically took screen shots of what was being displayed on the computer.

Attribution 1 Publication: databreaches.net / website Author:
Article Title: Center for Neurosurgical and Spinal Disorders discloses hack
Article URL: <https://www.databreaches.net/la-center-for-neurosurgical-and-spinal-disorders-discloses-hack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-13	Rotech Healthcare	FL	8/17/2016	Paper Data	Medical/Healthcare	Yes - Published #	957

On June 13, 2016, Rotech received a report that certain patient information had been recovered by law enforcement after being found in the possession of an unauthorized individual. Although the investigations into this incident by Rotech and law enforcement are ongoing, Rotech determined that the paper records recovered by law enforcement contained your personal and protected health information, including : name, Social Security number, patient number, address, the name of the Rotech subsidiary company from which you received health care services, and possibly phone number and/or date of birth.

Attribution 1 Publication: databreaches.net / hhs Author:
Article Title: Rotech Healthcare notifies patients whose details were found in possession of unauthorized individual
Article URL: <https://www.databreaches.net/rotech-healthcare-notifies-patients-whose-details-were-found-in-possession-of-unautho>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-12	University of New Mexico	NM	8/17/2016	Electronic	Educational	Yes - Published #	1,300

Ronald Murray is accused of taking personal information from a University of New Mexico database and using it to go on a nearly \$90,000 spending spree. Trujillo said Murray had a flash drive containing personal information for 1,300 former UNM students and employees. Police still don't know how he obtained it.

Attribution 1 Publication: koat.com Author:
Article Title: UNM students, employees could be victims of ID theft
Article URL: <http://www.koat.com/news/unm-students-employees-could-be-victims-of-id-theft/41256378>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-11	Eastern Carolina Cardiovascular / Outer Banks	NC	8/19/2016	Electronic	Medical/Healthcare	Yes - Published #	1,000

Personal data for patients over a period of 12 years might be at risk after two thumb drives went missing during the transfer of computer files from Eastern Carolina Cardiovascular to The Outer Banks Hospital.

Attribution 1 Publication: <http://outerbanksvoice.com/> Author: Rob Morris
Article Title: Hospital alerts cardio-rehab patients of data loss
Article URL: <http://outerbanksvoice.com/2016/08/19/hospital-alerts-cardio-rehab-patients-of-possible-data-loss/>

Attribution 2 Publication: databreaches.net / outbanksvoice.com Author:
Article Title: Hospital alerts cardio-rehab patients of data loss
Article URL: <http://outbanksvoice.com/2016/08/19/hospital-alerts-cardio-rehab-patients-of-possible-data-loss/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-10	Factory RV Surplus	IN	8/22/2016	Electronic	Business	Yes - Published #	8,500

More than one month ago, I was contacted by a consumer who was frustrated that Factory RV Surplus was exposing his information and that it had been indexed by Google. He called them and spoke to them, but nothing changed. He also contacted authorize.net, who also did nothing. In frustration, he turned to DataBreaches.net. This site attempted to contact the firm directly, but got no response. This site then contacted Digital Hill Media on July 25, as they are listed in the domain registration as the responsible Tech admin.

Attribution 1 Publication: databreaches.net Author:
Article Title: Consumer Caution: Factory RV Surplus exposing customer info
Article URL: <https://www.databreaches.net/consumer-caution-factory-rv-surplus-exposing-customer-info/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-09	Scan Health Plan	CA	8/23/2016	Electronic	Medical/Healthcare	Yes - Published #	87,069

On June 27, 2016 we learned that contact sheets, which are documents kept in a system used for sales purposes, had been accessed and possibly viewed for unauthorized purposes. We immediately began an investigation and brought in outside experts. We determined the unauthorized access occurred between March and June of 2016. While there is no indication that the information in this system has been used fraudulently, we needed to let you know that your information was in this system.

Attribution 1 Publication: databreaches.net Author:
Article Title: SCAN Health Plan notifying members of unauthorized access to their information
Article URL: <https://www.databreaches.net/scan-health-plan-notifying-members-of-unauthorized-access-to-their-information/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-08	Idaho Department of Fish and Game / Active Network	ID	8/24/2016	Electronic	Government/Military	Yes - Published #	788,064

I just hacked four websites and reported the security holes. Two of these were government websites. All of these websites pertain to one type of activity that requires registering PI. Each website is contained to one state. I got over six million pieces of personal information from these websites. This should make the news. I'll list the exact websites once the security hole is patched and/or it makes the news.

Attribution 1 Publication: spokesman.com Author:
Article Title: Idaho Fish & Game warns customers after news that data breach compromised personal info
Article URL: <http://www.spokesman.com/blogs/boise/2016/aug/26/idaho-fish-game-warns-customers-after-news-data-breach-comp>

Attribution 2 Publication: databreaches.net Author:
Article Title: Four states' fishing and hunting licensing sites hacked
Article URL: <https://www.databreaches.net/four-states-fishing-and-hunting-licensing-sites-hacked/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-07	Oregon Department of Fish and Wildlife / Active Network	OR	8/24/2016	Electronic	Government/Military	Yes - Published #	1,195,204

I just hacked four websites and reported the security holes. Two of these were government websites. All of these websites pertain to one type of activity that requires registering PI. Each website is contained to one state. I got over six million pieces of personal information from these websites. This should make the news. I'll list the exact websites once the security hole is patched and/or it makes the news. 1,195,204 – Oregon: Name, DOB, Address, and DL#. Some have email and/or phone.

Attribution 1 Publication: mailtribune.com Author:
Article Title: Possible ODFW license hack reveals how tax fraud can occur
Article URL: <http://www.mailtribune.com/article/20160826/NEWS/160829722>

Attribution 2 Publication: databreaches.net Author:
Article Title: Four states' fishing and hunting licensing sites hacked
Article URL: <https://www.databreaches.net/four-states-fishing-and-hunting-licensing-sites-hacked/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-06	Kentucky Department of Fish & Wildlife	KY	8/24/2016	Electronic	Government/Military	Yes - Published #	2,126,449

I just hacked four websites and reported the security holes. Two of these were government websites. All of these websites pertain to one type of activity that requires registering PI. Each website is contained to one state. I got over six million pieces of personal information from these websites. This should make the news. I'll list the exact websites once the security hole is patched and/or it makes the news. 2,126,449 – Kentucky: Name, DOB, Address, and Last Four Digits of SSN. Some have email and/or phone.

Attribution 1 Publication: databreaches.net Author:
Article Title: Four states' fishing and hunting licensing sites hacked
Article URL: <https://www.databreaches.net/four-states-fishing-and-hunting-licensing-sites-hacked/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-05	Washington Department of Fishing & Wildlife / Active	WA	6/15/2016	Electronic	Government/Military	Yes - Published #	2,435,452

It doesn't appear that a hacker or hackers was able to gain access to sensitive customer information in apparent cyber vandalism on WDFW's public website earlier this week, but it will be down for at least 24 more hours as techies check for vulnerabilities. 2,435,452 – Washington: Name, DOB, Address, DL#, Last Four Digits of SSN, Height, Weight, and Eye Color. Some have email and/or phone.

Attribution 1 Publication: northwestsportsman.com / databreaches Author:
Article Title: WDFW's Website Briefly Hacked, Unlikely Sensitive Info Accessed
Article URL: <http://nwsportsmanmag.com/editors-blog/wdfws-website-briefly-hacked-unlikely-sensitive-info-accessed/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-04	Epic Games	NC	8/23/2016	Electronic	Business	Yes - Unknown #	Unknown

Epic Games has temporarily shut down some of its user forums for maintenance after data on about 808,000 accounts was stolen, marking the second data breach of the game maker in 13 months.

Attribution 1 Publication: bankinfosecurity.com Author:
Article Title: Epic Games Forums Breached Again
Article URL: <http://www.bankinfosecurity.com/epic-games-forums-breached-again-a-9355>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-03	Dominican Hospital	CA	8/18/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On July 28, 2016, we discovered that a Microsoft Excel workbook was transmitted using our secured (encrypted) email system to a local health plan containing an excessive number of patients, some of whom may not be covered by or associated with the health plan.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Dominican Hospital
Article URL: https://oag.ca.gov/system/files/Patient%20Notifications%20-%20Scanned_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-02	Schwan's	MN	8/15/2016	Electronic	Business	Yes - Unknown #	Unknown

As part of CARDSource's investigation, it was determined that the potentially compromised data included the names of some of our Schwan'sPay customers, along with their mailing addresses, email addresses, phone numbers and Schwan'sPay card numbers.

Attribution 1 Publication: CA AG's office / OR AG's office Author:
Article Title: Schwan's
Article URL: https://oag.ca.gov/system/files/Customer%20Letter%20DB%20Templ%20Fin_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160824-01	Eddie Bauer, LLC	WA	8/18/2016	Electronic	Business	Yes - Published #	2,192,422

We recently learned that point of sale systems at Eddie Bauer retail stores may have been accessed without our authorization. We immediately initiated a full investigation with third-party digital forensic experts. On August 11, 2016 we received confirmation that your payment card information used at one or more of our retail stores may have been accessed without authorization. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
 Article Title: Eddie Bauer, LLC
 Article URL: https://oag.ca.gov/system/files/Eddie%20Bauer%20non-Massachusetts%20consumer%20notification%20final_1.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160817-01	Nevada Department of Transportation	NV	8/17/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

The personal information, including social security numbers, of state employees was breached and used to apply for state unemployment claims. That's according to the Nevada Department of Transportation which notified its employees yesterday of the security breach. "We want to make you aware that your Personal Identifiable Information (PII), including your name, date of birth, and Social Security Number may have been exposed," the government agency wrote to its employees. "This notification is intended to provide you with information which may assist you in preventing or responding to fraudulent use of your PII."

Attribution 1 Publication: thisisreno.com Author:
 Article Title: Data Breach Exposes Personal Information Of State Employees
 Article URL: <http://thisisreno.com/2016/08/data-breach-exposes-personal-information-state-employees/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160816-06	Shoppe Designs	CA	8/15/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 24th we received an email from Meghan Aileen, the original owner of TheShoppeDesigns.com, telling us she had received an email from a developer that helped her create the site. He had uncovered a hack being used to steal information from many websites using the Lemonstandv1 e-commerce platform.

Attribution 1 Publication: NH AG's office Author:
 Article Title: Shoppe Designs
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/the-shoppe-designs-20160815.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160816-05	FSC Securities Corporation	GA	8/10/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On May 24, 2016, an FSC became aware of several fraud attempts against clients from the same FSC branch office (none of whom were NH residents), which led to an investigation to find the cause. We believe there was a cybersecurity event; however the precise source could not be determined with certainty.

Attribution 1 Publication: NH AG's office Author:
 Article Title: FSC Securities Corporation
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/fsc-securities-20160810.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160816-04	First Home Mortgage Corp.	MD	8/12/2016	Electronic	Banking/Credit/Financial	Yes - Published #	1,300

On July 10, 2016, a First Home employee had his vehicle broken into and his company laptop stolen. Although the computer was password protected and it is unlikely that the stored data was accessed, First Home believes that certain customer information, address, Social Security number, driver's license or identification number, and financial account number may have been stored on this device and could have potentially been affected as a result of the theft. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: First Home Mortgage Corp.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/first-home-mortgage-20160812.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160816-03	EBSCO Industries, Inc.	AL	8/9/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently became aware of a malware intrusion affecting our e-commerce platform by targeting customers' payment card information. We estimate that the malware operated between July 16 and July 22, 2016 by intercepting payment card information entered into our ecommerce accessed included personal information such as names, billing addresses, email addresses and credit card numbers (including CCV numbers).

Attribution 1 Publication: NH AG's office Author:
Article Title: EBSCO Industries, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/ebSCO-industries-20160809.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160816-02	Neurology Physicians LLC	MD	7/20/2016	Electronic	Medical/Healthcare	Yes - Published #	4,831

Neurology Physicians LLC MD Healthcare Provider 4831 07/20/2016 Hacking/IT IncidentOther

Attribution 1 Publication: hhs.gov Author:
Article Title: Neurology Physicians LLC
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-01	Autism Home Support Services	IL	8/10/2016	Electronic	Medical/Healthcare	Yes - Published #	533

Autism Home Support Services IL Healthcare Provider 533 08/10/2016 Unauthorized Access/DisclosureEmail

Attribution 1 Publication: hhs.gov Author:
Article Title: Autism Home Support Services
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-11	County of Anderson	TN	8/10/2016	Electronic	Government/Military	Yes - Published #	1,800

County Law Director Jay Yeager sent a memo to all elected officials, school system employees, school board members, veterans service members and county contractors that there had been a "potential system-wide breach" of the main courthouse server. Yeager says about 1,800 people have been notified they may be affected.

Attribution 1 Publication: Knoxville News Sentinel Author: Lynda Edwards
Article Title: Still no answers in Anderson County courthouse server hack
Article URL: <http://www.knoxnews.com/news/state/still-no-answers-in-anderson-county-courthouse-server-hack-3c799227-ae71-56>

Attribution 2 Publication: databreaches.net / WATE.com Author:
Article Title: 1,800 possibly affected by Anderson County government computer breach
Article URL: <https://www.databreaches.net/tn-1800-possibly-affected-by-anderson-county-government-computer-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-10	EXOS (Athletes' Performance)	AZ	8/10/2016	Electronic	Medical/Healthcare	Yes - Published #	854

Recently, we learned that the laptop of an EXOS employee was stolen from our facility. While, typically, laptops are not stolen to access the data on the laptop, we would like you to know that your personal information, including name, contact information, payment data, health information and/or insurance information, may have been on the stolen laptop.

Attribution 1 Publication: databreaches.net Author:
Article Title: Laptop stolen from EXOS contained protected health information
Article URL: <https://www.databreaches.net/az-laptop-stolen-from-exos-contained-protected-health-information/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-09	Department of State Health Services	TX	8/11/2016	Electronic	Government/Military	Yes - Published #	1,500

The missing book — one of about 800 volumes of birth records that state workers assemble each year from data passed on by local registrars — contained sensitive personal information on about 1,500 infants and parents, including the parents' Social Security numbers, Department of State Health Services spokeswoman Carrie Williams said Wednesday.

Attribution 1 Publication: Dallas Morning News Author:
Article Title: 2 officials sacked for not reporting loss of birth records that could have exposed 1,500 Texans to ID theft
Article URL: <http://www.dallasnews.com/news/politics/headlines/20160811-2-officials-sacked-for-not-reporting-loss-of-birth-record>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-08	University of Vermont	VT	8/10/2016	Electronic	Educational	Yes - Unknown #	Unknown

On July 1, 2016, we discovered that your UVM NetID and password were used to gain access to UVM's Human Resources People Soft Self-Service Module. Our investigation revealed that the unauthorized access, affecting a small number of employees, was the result of compromised UVM credentials for each affected employee (UVM NetID and password), which appear to have been stolen as part of a "phishing" scam. The email may have contained the subject "Message from UVM Staff Portal" or it could have contained a link that infected the computer you were using with malicious software.

Attribution 1 Publication: VT AG's office Author:
Article Title: University of Vermont
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/University%20of%20Vermont%20SBN%20to%20Consu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-07	Office of John E. Gonzalez, DDS	CA	7/25/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On the late afternoon of Monday July 25, 2016, my car window was broken out and my briefcase was stolen. In that briefcase was an external hard drive containing two different types of data. First, all office patient records were backed up on the drive, including social security numbers, driver's license numbers, phone numbers, date of birth, physical and email addresses and health insurance information.

Attribution 1 Publication: CA AG's office Author:
Article Title: Office of John E. Gonzalez, DDS
Article URL: https://oag.ca.gov/system/files/GONZALEZ%20breach%20letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-06	Valley Anesthesiology and Pain Consultants	AZ	8/12/2016	Electronic	Medical/Healthcare	Yes - Published #	882,590

On June 13, 2016, VAPC learned that a third party may have gained unauthorized access to VAPC computer systems on March 30, 2016. The computer systems may contain patient information, such as patient names, their providers' names, dates of service, places of treatment, names of health insurers, insurance identification numbers, diagnosis and treatment codes, and in some instances, social security numbers

Attribution 1 Publication: CA AG's office / company website Author:
Article Title: Valley Anesthesiology and Pain Consultants Notifying 882,590 Patients PLUS all Employees and Providers of Security Incident
Article URL: <https://www.databreaches.net/valley-anesthesiology-and-pain-consultants-notifying-882590-patients-plus-all-employee>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-05	Bon Secours Health Systems / R-C Healthcare Management	MD	4/18/2016	Electronic	Medical/Healthcare	Yes - Published #	655,203

Personal information of more than 650,000 Bon Secours patients – including names, insurance identification numbers, banking information, social security numbers and some clinical data – was left exposed on the internet for four days this spring by a business associate of the hospital system.

Attribution 1 Publication: Healthcareitnews.com / CA AG's office Author:
Article Title: Bon Secours says data breach affects 655,000 patients
Article URL: <http://www.healthcareitnews.com/news/bon-secours-says-data-breach-affects-655000-patients>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-04	HEI Hotels & Resorts	CT	6/21/2016	Electronic	Business	Yes - Unknown #	Unknown

According to HEI, "unauthorized individuals" installed malware on its payment processing systems at these properties that can capture payment card information at the point of purchase.

Attribution 1 Publication: usatoday.com / CA AG's office Author:
Article Title: Hotel operator hit by data breach
Article URL: <http://www.usatoday.com/story/tech/news/2016/08/15/major-hotel-operator-hit-data-breach/88753160/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-03	PAX Labs, Inc.	CA	8/12/2016	Electronic	Business	Yes - Published #	6,036

On July 15, 2016, we discovered that an unauthorized party had gained access to one of our cloud-based website servers and installed unauthorized software. PAX removed this software on July 15, 2016. Subsequently, an unauthorized party added similar software on July 22, 2016, which PAX removed that same day. Our investigation revealed that the unauthorized party accessed personal payment card information of approximately 6,000 customers who had made purchases from either www.JUULvapor.com or www.PAXvapor.com between June 25, 2016, and July 22, 2016. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / IN AG' Author:
Article Title: PAX Labs, Inc.
Article URL: https://oag.ca.gov/system/files/PAX%20-%20Consumer%20Data%20Breach%20Notice_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-02	Office of Brian Halevie-Goldman, MD	CA	7/19/2016	Electronic	Medical/Healthcare	Yes - Published #	2,000

On July 19, 2016 two laptop computers belonging to the medical offices of Dr. Brian Halevie-Goldman were stolen. The laptops were password protected, secured in a carrying case and locked inside a vehicle when the theft occurred.

Attribution 1 Publication: CA AG's office / databreaches.net / hipa Author:
Article Title: Office of Brian Halevie-Goldman, MD
Article URL: https://oag.ca.gov/system/files/breach%20%20letter%20pdf_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160815-01	7-Eleven, Inc.	CA	6/13/2016	Electronic	Business	Yes - Published #	7,832

7-Eleven discovered in June 2016 that as part of the update process, in addition to the normal set of employee records sent for each Employing Franchisee, some additional records from the franchisee employee database were available to certain 7-Eleven franchisees. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: 7-Eleven, Inc.
Article URL: https://oag.ca.gov/system/files/Individual%20notice%20-%20SAMPLE_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160810-02	FDIC #2	DC	8/10/2016	Electronic	Government/Military	Yes - Published #	30,000

Occurring in New York On or about September 29, 2015, the FDIC learned that a poor performing and disgruntled employee in New York returned all electronic devices when she left her job at FDIC, with the exception of a portable USB device containing sensitive resolution plans, commonly known as living wills, sensitive banking information, and the social security numbers of 28,000-30,000 individuals.

Attribution 1 Publication: GOP Interim Staff Report Author:
Article Title: FDIC #2
Article URL: <file:///S:/Final%20GOP%20Interim%20Staff%20Report%207-12-16.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-09	Santander	MA	8/1/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On July 17, 2016, the Santander Bank Fraud Card Detection group discovered suspicious ATM withdrawals that occurred that day. The personal information potentially compromised included the customer's name, card number, card expiration date, card security code, and card PIN numbers.

Attribution 1 Publication: NH AG's office Author:
Article Title: Santander
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/santander-20160801.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-08	KGA, Inc.	MA	8/1/2016	Electronic	Business	Yes - Unknown #	Unknown

On July 6, 2016, KGA discovered that an employee was the subject of a phishing attack when the employee received an email purporting to be from the Chairman that, after the exchange of several emails, requested a wire transfer of funds. KGA immediately began an investigation, discovered that the employee's email account had been previously accessed by an unknown intruder, and determined that the request did not come from the Chairman, but from an unknown e-mail address that was made to appear to be the Chairman's email address.

Attribution 1 Publication: NH AG's office Author:
Article Title: KGA, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/kga-20160801.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-07	Primoris Services Corporation / Hein &	CO	7/13/2016	Electronic	Business	Yes - Unknown #	Unknown

On June 13, 2016, Hein learned that certain personal information on the laptop may have been accessible. Hein has confirmed that the laptop that was stolen contained electronic files with employee names and Social Security numbers of one of its clients, TransMontaigne. Although the laptop was encrypted, Hein is concerned that information on the computer may be accessible.

Attribution 1 Publication: MT AG's office Author:
Article Title: Primoris Services Corporation / Hein & Associates LLP
Article URL: <https://dojmt.gov/wp-content/uploads/Primoris-Services-Corporation.pdf>

Attribution 2 Publication: NH AG's office Author:
Article Title: Primoris Services Corporation / Hein & Associates LLP
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/hein-associates-20160713.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-06	Carle Foundation Hospital	IL	8/8/2016	Electronic	Medical/Healthcare	Yes - Published #	1,185

Carle Foundation Hospital in Urbana, Ill., is notifying patients of a data breach stemming from a hospital vendor, according to The News-Gazette. One of Carle's vendors reportedly placed files containing 1,185 patients' medical records on a server intended to share large documents, according to the report. The incident took place Feb. 17.

Attribution 1 Publication: beckershospitalreview.com / hipaajourna Author:
Article Title: Carle Foundation Hospital breach affects 1,185 patients
Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/carle-foundation-hospital-breach-affects-1->

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 106 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-04	Professional Dermatology Care, PC	VA	8/9/2016	Electronic	Medical/Healthcare	Yes - Published #	13,237

On June 27, 2016, Professional Dermatology Care, P.C. (PDC, P.C.) discovered a potential data breach of its network server. Following a comprehensive cybersecurity and forensic investigation, PDC, P.C. learned that unauthorized third parties from outside the United States may have recently accessed and obtained patient protected health information and financial data between June 19, 2016 and June 27, 2016.

Attribution 1 Publication: [hhs.gov / databreaches.net / company w](http://hhs.gov/databreaches.net/company-w) Author:
Article Title: Professional Dermatology Care, PC
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-03	TD Bank	NJ	8/8/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently determined a privacy issue occurred. We're making things right. We recently learned that your personal information may have been inappropriately accessed by one of our employees without a legitimate business need. The personal information accessed may have included your name, address, date of birth, social security number, and account number.

Attribution 1 Publication: VT AG's office Author:
Article Title: TD Bank
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/TD%20Bank%20NA%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-02	MedAltus. LLC	NY	8/8/2016	Electronic	Business	Yes - Unknown #	Unknown

Beginning at least as early as May 3, 2016, we believe MedAltus order information may have been improperly intercepted/accessed from our Ecommerce website. This order information may have included your name, address, email, phone number, fax number, credit card information and any username or password that you may have created to access the site and purchase products. As a result, this information may have been potentially exposed to others.

Attribution 1 Publication: VT AG's office Author:
Article Title: MedAltus. LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/MedAltus.%20LLC%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160809-01	Travelon	IL	8/4/2016	Electronic	Business	Yes - Published #	1,672

Based on what we currently know, between November 13, 2015 and June 10, 2016, malicious code was placed on Travelon's server that caused the collection of data that was inputted in the shopping cart application on Travelon's website for transmission to the credit card processing vendor. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / IN AG's Author:
Article Title: Travelon
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Travelon%20-%20Travel%20Caddy%20Inc%20SBN%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160808-02	Newkirk Products	NY	8/8/2016	Electronic	Medical/Healthcare	Yes - Published #	3,466,120

A security breach at a company that supplies identification cards for health insurance companies may expose the personal information of about 3.3 million people, including those covered by Albany-based Capital District Physicians' Health Plan and Latham-based BlueShield of Northeastern New York, as well as about a dozen other organizations. The company, Albany-based Newkirk Products, posted a notice about the breach on its website Friday. Information on the ID cards of more than a half million CDPHP members and about 70,000 BlueShield members was potentially accessed. The information on these cards included name, mailing address, type of plan, subscriber and group ID number, and names of covered dependents.

Attribution 1 Publication: timesunion.com Author:
Article Title: Data breach at Albany firm may affect CDPHP, BlueShield members
Article URL: <http://www.timesunion.com/local/article/Data-breach-at-Albany-firm-may-affect-CDPHP-9129259.php>

Attribution 2 Publication: hipaajournal.com Author:
Article Title: 3.3 MILLION RECORD BREACH REPORTED BY BCBS VENDOR
Article URL: <http://www.hipaajournal.com/3-3-million-record-breach-reported-bcbs-vendor-3538/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160808-01	Oracle - MICROS	CA	8/8/2016	Electronic	Business	Yes - Unknown #	Unknown

A Russian organized cybercrime group known for hacking into banks and retailers appears to have breached hundreds of computer systems at software giant Oracle Corp., KrebsOnSecurity has learned. More alarmingly, the attackers have compromised a customer support portal for companies using Oracle's MICROS point-of-sale credit card payment systems.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Data Breach At Oracle's MICROS Point-of-Sale Division
Article URL: <https://krebsonsecurity.com/2016/08/data-breach-at-oracles-micros-point-of-sale-division/>

Attribution 2 Publication: techtimes.com Author: Dianne Depra
Article Title: Oracle Confirms Data Breach Involving MICROS Point-Of-Sale Systems
Article URL: <http://www.techtimes.com/articles/173228/20160810/oracle-confirms-data-breach-involving-micros-point-of-sale-systems>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160805-01	Banner Health	AZ	8/5/2016	Electronic	Medical/Healthcare	Yes - Published #	3,623,140

On July 7, the company discovered that hackers may have accessed computer systems that process payment card data at food and beverage locations at some Banner Health facilities, potentially exposing the names, card numbers, expiration dates and verification codes for those who used payment cards at Banner Health food and beverage locations between June 23 and July 7, 2016.

Attribution 1 Publication: eSecurity Planet / CA AG's office Author: Jeff Goldman
Article Title: 3.7 Million People Affected by Massive Data Breach at Banner Health
Article URL: <http://www.esecurityplanet.com/hackers/3.7-million-people-affected-by-massive-data-breach-at-banner-health.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-33	Institute of Management Accountants	NJ	7/19/2016	Electronic	Business	Yes - Unknown #	Unknown

IMA was informed on June 20, 2016, that one of its vendors, Comnet Marketing Group, Inc. ("Comnet"), had been the victim of an intrusion of its computer systems. An unauthorized user gained administrative access to Comnet's systems on April 23-24, 2016, and issued commands to delete all the data housed on Comnet's servers.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Institute of Management Accountants
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/ima-20160719.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-32	Comnet Marketing Group	OR	7/22/2016	Electronic	Business	Yes - Unknown #	Unknown

On or around April 22, 2016, Comnet was the victim of a ransomware attack. While investigating this incident, on April 24, 2016, Comnet suffered a failure of its storage system that housed sensitive data.

Attribution 1 Publication: OR AG's office Author:
Article Title: Comnet Marketing Group
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1174305394>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 108 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-31	Tax Shack	WA	6/16/2016	Electronic	Business	Yes - Unknown #	Unknown

Sometime over Memorial Day weekend, someone broke through the 2' x 2' glass window at our principal place of business and stole our safety deposit box and petty cash. Upon discovery of the incident, and after a thorough investigation, we determined that none of our clients' files, or Company files, computers, notes, etc. were tampered with or taken.

Attribution 1 Publication: WA AG's office Author:
Article Title: Tax Shack
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/TheTaxShack.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-30	NLU Products / BGZ Brands	UT	7/17/2016	Electronic	Business	Yes - Published #	114,261

We recently discovered that we have been the victim of a data security incident that began in April 2015, during which personal, private and unencrypted credit/debit card information may have been exposed to an outside party and compromised. (Consumers affected per IN AG's office)

Attribution 1 Publication: WA AG's office / SC AG's office / IN AG' Author:
Article Title: NLU Products / BGZ Brands
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/NLUProductsLLC.p

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-29	Academy of Nutrition and Dietetics	IL	7/28/2016	Electronic	Business	Yes - Unknown #	Unknown

On June 17, 2016, the Telemarketer notified the Academy that the Telemarketer had been the victim of a ransomware attack on its computer systems. The Telemarketer advised the Academy the attack on their systems took place on April 22, 2016 and lasted until April 24, 2016. The Telemarketer has advised the Academy that as part of the attack they believe the attackers may have gained unauthorized access to the Telemarketer's computer systems that contained some of your personal information.

Attribution 1 Publication: VT AG's office Author:
Article Title: Academy of Nutrition and Dietetics
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Academy%20of%20Nutrition%20and%20Dietetics%20S

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-28	American Society of Safety Engineers	IL	7/20/2016	Electronic	Business	Yes - Unknown #	Unknown

On June 17, 2016, the Telemarketer notified ASSE that the Telemarketer had been the victim of a ransomware attack on its computer systems. The Telemarketer advised ASSE the attack on their systems took place on April 22, 2016 and lasted until April 24, 2016. The Telemarketer has advised ASSE that as part of the attack they believe the attackers may have gained unauthorized access to the Telemarketer's computer systems that contained some of your personal information.

Attribution 1 Publication: VT AG's office Author:
Article Title: American Society of Safety Engineers
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/American%20Society%20of%20Safety%20Engineers%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-27	Internet Chess Club	PA	7/19/2016	Electronic	Business	Yes - Published #	1,651

A portion of the Internet Chess Club website was attacked by malware that made it possible for customer purchase information to be scraped from the ICC website. The malware was launched on approximately April 1, 2016. It was discovered in late May, 2016, and the vulnerability was immediately repaired. However, as a result of this vulnerability, it is possible that customer transaction records were gathered by an external hacker. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / IN AG's office Author:
Article Title: Internet Chess Club
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Internet%20Chess%20Club%20SBN%20to%20Consum

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 109 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-26	inVentiv Health	MA	6/2/2016	Electronic	Medical/Healthcare	Yes - Published #	14,604

On July 7, 2016, we learned that a targeted “phishing” email message had been sent to inVentiv Health in June. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. The email was designed to appear as though it had been sent by an inVentiv executive, from the inVentiv executive’s email account, requesting the uploading of our U.S. employees’ 2015 W-2 Forms to a file sharing site. Believing the email request to be legitimate, the W-2 data was uploaded. It is unknown how much of the data uploaded may have been accessed by unauthorized individuals. (Consumers affected per IN AG’s office)

Attribution 1 Publication: CA AG’s office / MD AG’s office / IN AG’ Author:
Article Title: inVentiv Health
Article URL: https://oag.ca.gov/system/files/inVentiv%20CA%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-24	Democratic Political Organizations	DC	7/29/2016	Electronic	Business	Yes - Unknown #	Unknown

A computer network used by Democratic presidential nominee Hillary Clinton’s campaign was hacked as part of a broad cyber attack on Democratic political organizations, people familiar with the matter told Reuters.

Attribution 1 Publication: Reuters.com Author:
Article Title: Exclusive: Clinton campaign also hacked in attacks on Democrats
Article URL: <http://www.reuters.com/article/us-usa-cyber-democrats-investigation-exc-idUSKCN1092HK>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-23	Office of Ceaton C. Falgiano	NY	6/27/2016	Electronic	Medical/Healthcare	Yes - Published #	650

Ceaton C Falgiano NY Healthcare Provider 650 06/27/2016 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Ceaton C. Falgiano
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-22	Heart Center of Southern Maryland, LLP	MD	7/7/2016	Electronic	Medical/Healthcare	Yes - Published #	1,350

Heart Center of Southern Maryland, L.L.P. MD Healthcare Provider 1350 07/07/2016 Hacking/IT Incident Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: Heart Center of Southern Maryland, LLP
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-21	Cefalu Eye-Tech of Green, Inc.	OH	7/14/2016	Electronic	Medical/Healthcare	Yes - Published #	850

An employee of Cefalu Eye-Tech of Green, Inc. (Cefalu) photographed computer screens containing the protected health information (PHI) of approximately 850 individuals, including names, addresses, email addresses, and codes for diagnosis and conditions. Following the breach, Cefalu investigated the breach and provided breach notification to HHS and the affected individuals. OCR determined that the reporting entity is no longer a covered entity.

Attribution 1 Publication: hhs.gov / databreaches.net Author:
Article Title: Cefalu Eye-Tech of Green, Inc.
Article URL: <https://www.databreaches.net/details-emerge-on-cefalu-eye-tech-of-green-breach/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 110 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-20	Sunshine State Health Plan, Inc.	FL	7/14/2016	Electronic	Medical/Healthcare	Yes - Published #	1,479
SUNSHINE STATE HEALTH PLAN, INC. FL Health Plan 1479 07/14/2016 Unauthorized Access/Disclosure Email							

Attribution 1 Publication: hhs.gov Author:
Article Title: Sunshine State Health Plan, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-19	Caring for Women, P.A.	TX	7/22/2016	Electronic	Medical/Healthcare	Yes - Published #	697
Caring for Women, PA TX Healthcare Provider 697 07/22/2016 Unauthorized Access/Disclosure Email							

Attribution 1 Publication: hhs.gov Author:
Article Title: Caring for Women, P.A.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-18	Greenville Health System (Carolina Cardiology) /	DE	7/22/2016	Electronic	Medical/Healthcare	Yes - Published #	2,500
Back in July, Ambucor Health Solutions reported a breach to HHS that affected 1,679 patients. Their report, submitted as a Business Associate, was coded as "Unauthorized Access/Disclosure – Email," with the location of the data being "Other Portable Electronic Device." That incident was included in Protenus's breach barometer for July, but no additional details were available at that time.							

Attribution 1 Publication: hhs.gov / databreaches.net Author:
Article Title: Business associate breach affected Greenville Health System patients
Article URL: <https://www.databreaches.net/business-associate-breach-affected-greenville-health-system-patients/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-17	Premier Family Care / Mario M. Gross M.D.	TX	7/25/2016	Electronic	Medical/Healthcare	Yes - Published #	1,326
On April 8, 2016, unsupervised medical records were discovered in the former home of Dr. Mario Gross, who was previously an employee of Premier Physicians. The doctor had moved out of the local area and left behind files and records, which remained in his house after possession transferred to a local bank. Recognizing that the records had been left unattended, we immediately removed and secured the patient files and initiated a thorough examination to determine what information was contained in the records. The examination determined that the records contained a variety of patient information including names, dates of birth, medical record numbers, Social Security numbers, clinical data, and medical insurance information. The records did not include any credit or payment card information.							

Attribution 1 Publication: databreaches.net / company website Author:
Article Title: Premier Physicians Notifies Patients of Records Security Incident
Article URL: <http://yourpremierphysicians.com/recordsincident.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-16	StarCare Specialty Health System	TX	7/26/2016	Electronic	Medical/Healthcare	Yes - Published #	2,900
On Monday, May 30, 2016 StarCare discovered that one or more people broke into a StarCare/StarQuest office at 3315 East Broadway in Lubbock, Texas. Five lap-top computers were stolen from the office. Only one laptop had confidential information that the burglar can access. The affected laptop was disabled to reduce any harm. Additionally, one box of paper files may have been viewed by the suspect.							

Attribution 1 Publication: databreaches.net / company website Author:
Article Title: StarCare Specialty Health System notifies patients after burglar snatches laptop, paper files
Article URL: <https://www.databreaches.net/tx-starcare-specialty-health-system-notifies-patients-after-burglar-snatches-laptop-pape>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-15	Kimpton Hotels	CA	7/26/2016	Electronic	Business	Yes - Unknown #	Unknown

Kimpton Hotels, a boutique hotel brand that includes 62 properties across the United States, said today it is investigating reports of a credit card breach at multiple locations. On July 22, KrebsOnSecurity reached out to San Francisco-based Kimpton after hearing from three different sources in the financial industry about a pattern of card fraud that suggested a card breach at close to two-dozen Kimpton hotels across the country.

Attribution 1 Publication: infosecourcemagazine / NH AG's office / Author:
Article Title: Kimpton Hotels Hit with 6-Month Card Data Breach
Article URL: <http://www.infosecurity-magazine.com/news/kimpton-hotels-hit-6-month-card/>

Attribution 2 Publication: krebsonsecurity.com Author:
Article Title: Kimpton Hotels Probes Card Breach Claims
Article URL: <http://krebsonsecurity.com/2016/07/kimpton-hotels-probes-card-breach-claims/-more-35647>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-14	Midwest Orthopedics Group	MO	7/27/2016	Electronic	Medical/Healthcare	Yes - Published #	29,153

"We write to inform you that our practice discovered a data breach on May 27, 2016 that may have contained personal health information and have been investigating the exact nature and scope of the information obtained by the hackers since," the letter reads. "To date, our investigation has determined that on May 4, 2016, a hacker, or hackers, likely gained access into our secured database system through a third party contractor and may have obtained some personal information of our patients including: names, addresses, social security numbers, date of births, diagnoses, lab results, other medical records, and potentially some financial information."

Attribution 1 Publication: hipaajournal.com Author:
Article Title: FARMINGTON MEDICAL GROUP CONFIRMS CYBERATTACK
Article URL: <http://www.hipaajournal.com/farmington-medical-group-confirms-cyberattack-3527/>

Attribution 2 Publication: databreaches.net / dailyjournalonline.co Author:
Article Title: Local medical group involved in computer hack identified
Article URL: http://dailyjournalonline.com/news/local/local-medical-group-involved-in-computer-hack-identified/article_1dfafa55-d3

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-13	Athens Orthopedic Clinic	GA	7/27/2016	Electronic	Medical/Healthcare	Yes - Published #	201,000

Athens Orthopedic Clinic recently experienced a data breach due to an external cyber-attack on our electronic medical records using the credentials of a third-party vendor. Personal information of our current and former patients has been breached, including names, addresses, social security numbers, dates of birth and telephone numbers, and in some cases diagnoses and partial medical history.

Attribution 1 Publication: databreaches.net / AOC website Author:
Article Title: Athens Orthopedic Clinic to begin notifying patients of hack (UPDATE2)
Article URL: <https://www.databreaches.net/athens-orthopedic-clinic-to-begin-notifying-patients-of-hack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-12	Memorial Hermann	TX	7/20/2016	Electronic	Medical/Healthcare	Yes - Published #	12,061

Memorial Hermann Wednesday announced an incident involving the disclosure of protected health information to select primary care physicians. The company said the information disclosed was limited to the member's demographic information, that no medical information was disclosed. A Memorial Hermann employee on May 16 reported potential improper use of her PHI to the Memorial Hermann Privacy Office after the employee received a letter from a PCP she had no prior relationship with regarding the need for an annual physical.

Attribution 1 Publication: databreaches.net / click2houston.com Author:
Article Title: Memorial Hermann notifies employees of privacy incident
Article URL: <http://www.click2houston.com/news/memorial-hermann-notifies-employees-of-privacy-incident>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-11	Lifewellness Institute / Bizmatics	CA	7/29/2016	Electronic	Medical/Healthcare	Yes - Published #	2,473

We're still learning of other Bizmatics clients who were notified that their patient data may have been acquired by criminals. Lifewellness Institute in California notified HHS this month that they had notified 2,473 of their patients of the incident.

Attribution 1 Publication: databreaches.net Author:
Article Title: Another Bizmatics client notifies patients of breach
Article URL: <https://www.databreaches.net/another-bizmatics-client-notifies-patients-of-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-10	Jefferson Medical Associates	MS	7/29/2016	Electronic	Medical/Healthcare	Yes - Published #	10,401

On approximately June 1, 2016, an unauthorized individual not affiliated with JMA accessed a database containing a limited history of prescriptions and other information for a small percentage of patients. Based on the investigation so far, it appears that the individual unlawfully accessed and copied one of the practice's databases which included patient names, dates of birth, social security numbers, addresses, and phone numbers, as well as limited prescription information associated with their treatment at JMA, including drug names, dosages, and refill quantities.

Attribution 1 Publication: databreaches.net / company website / M Author:
Article Title: Jefferson Medical Associates notifies patients of new and old breaches
Article URL: <http://www.jeffersonmedical.net/breach/index.php>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-09	Prosthetic & Orthotic Care	MO	7/29/2016	Electronic	Medical/Healthcare	Yes - Published #	23,015

Exploiting a previously-unknown flaw in software purchased by P&O Care, the thieves obtained patient medical records that include names, contact information, P&O Care patient ID numbers, diagnostic codes, appointment dates and last billing amounts. Some records also contain Social Security numbers, birth dates, medical insurance company, and identification information and photos of procedures.

Attribution 1 Publication: databreaches.net / company website Author:
Article Title: Prosthetic & Orthotic Care confirms hack by TheDarkOverlord
Article URL: <https://www.databreaches.net/another-victim-of-thedarkoverlord-confirms-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-08	Crozer-Keystone Health System / Center for Minimally	PA	7/29/2016	Electronic	Medical/Healthcare	Yes - Published #	900

On June 20, 2016, we learned that a CKHS employee sent an email that same day to some patients in our Crozer-Keystone Comprehensive Bariatric Surgery Program regarding a support group for those patients. The email addresses were inadvertently placed in the "Cc" section of the email, instead of the "Bcc" or blind carbon copy section, making the email addresses of the recipients visible.

Attribution 1 Publication: databreaches.net / company website Author:
Article Title: Bariatric patients' privacy was compromised, Crozer-Keystone says
Article URL: <https://www.databreaches.net/pa-bariatric-patients-privacy-was-compromised-crozer-keystone-says/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-07	University of North Carolina - Charlotte	NC	7/29/2016	Electronic	Educational	Yes - Unknown #	Unknown

UNC Charlotte employees' bank accounts were targeted by a hacker. The school was alerted to the breach when it found a problem with an employee's direct deposit information.

Attribution 1 Publication: databreaches.net / WSOctv.com Author:
Article Title: UNC Charlotte employees bank accounts hacked
Article URL: <http://www.wsocv.com/news/local/potential-email-scam-at-uncc-affecting-direct-deposit-info/413523311>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-06	University of Arkansas for Medical Sciences	AR	7/30/2016	Electronic	Medical/Healthcare	Yes - Published #	42

Around January 6, 2016, UAMS became aware that a box containing medical records of some patients who received services and treatment at UAMS Child Study Center was missing. In retrieving a patient's medical record from storage, it was discovered that the records of 42 patients were missing.

Attribution 1 Publication: [databreaches.net](#) Author:
Article Title: University of Arkansas for Medical Sciences statement on missing patient records
Article URL: <https://www.databreaches.net/university-of-arkansas-for-medical-sciences-statement-on-missing-patient-records/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-05	Disney Consumer Products / Playdom Forum	CA	7/30/2016	Electronic	Business	Yes - Unknown #	Unknown

The investigation found that an unauthorized party obtained usernames, passwords and email addresses for approximately 391,000 playdomforums.com accounts. The unauthorized party also obtained the Internet Protocol (IP) address collected during user registration on playdomforums.com. The Playdom Forum website does not collect credit card numbers or other sensitive personal information, such as Social Security numbers.

Attribution 1 Publication: [databreaches.net](#) Author:
Article Title: Playdom Forum Site Breach Affects 391,000 : Usernames, Email Addresses and Passwords Impacted
Article URL: <https://www.databreaches.net/playdom-forum-site-breach-affects-391000-usernames-email-addresses-and-passwords->

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-04	Access Health Care Physicians	FL	7/31/2016	Electronic	Medical/Healthcare	Yes - Published #	2,500

Break-in leaves 2,000 patients' personal information at risk. Access Health Care Physicians has notified approximately 2,000 patients of a breach of unsecured personal patient protected health information following a break-in at the medical office of Dr. Imad Tarabishy, 11339 Cortez Blvd., Brooksville.

Attribution 1 Publication: [databreaches.net / tambabay.com](#) Author:
Article Title: Access Health Care Physicians
Article URL: <http://www.tampabay.com/news/briefs/hernando-briefs-for-july-22/2286120>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-03	Blaine Chiropractic Center	MN	7/31/2016	Electronic	Medical/Healthcare	Yes - Published #	1,945

On May 14, 2016, we discovered unauthorized software installed by an unknown person using a hidden administrator account. During our investigation, it was discovered that the administrator account had been created and subsequently made hidden by our third party software vendor at the point of installation of our patient record software. It is not known whether any patient information was in fact accessed. Information that could possibly have been accessed includes names, addresses, telephone number, email address, appointment activity, clinical care notes, insurance information, and social security numbers.

Attribution 1 Publication: [databreaches.net / hhs.gov](#) Author:
Article Title: Blaine Chiropractic Center
Article URL: <https://www.databreaches.net/some-recent-additions-to-hhss-breach-tool/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-02	American Family Care	AL	8/1/2016	Electronic	Medical/Healthcare	Yes - Published #	7,200

Despite that commitment, an issue was recently discovered that led to the unintentional release of protected health information ("PHI"). The issue involved x-ray CDs that were provided to patients at AFC's Alabaster, Flintridge, and Wetumpka, Alabama clinics, and Smyrna, Tennessee clinic, between the dates of August 26, 2015, through June 14, 2016. Due to an error in the design and installation of third-party software, discs were released containing the following PHI: patient name; date of birth, patient gender, and patient identification number. However, information such as social security numbers, driver's license numbers, financial data, and home addresses were not included on the CDs.

Attribution 1 Publication: [hhs.gov / databreaches.net](http://hhs.gov/databreaches.net) Author:
Article Title: American Family Care notifies 7,200 patients of breach involving PHI
Article URL: <https://www.databreaches.net/american-family-care-notifies-7200-patients-of-breach-involving-phi/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160802-01	Central Ohio Urology Group	OH	8/2/2016	Electronic	Medical/Healthcare	Yes - Published #	300,000

On August 2, 2016, an unauthorized individual posted files and documents to an online drive accessible on the Internet, which included personal information about patients, employees, and other individuals. The posted information appears to have been maintained by Central Ohio Urology Group on its internal file server.

Attribution 1 Publication: [databreaches.net / NH AG's office](http://databreaches.net) Author:
Article Title: DEVELOPING: Central Ohio Urology Group hacked, PHI dumped: hacktivist
Article URL: <https://www.databreaches.net/developing-central-ohio-urology-group-hacked-phi-dumped-hacktivist/>

Attribution 2 Publication: [NH AG's office / hipaajournal.com](http://nhag.org) Author:
Article Title: Central Ohio Urology Group
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/central-ohio-urology-20160922.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160727-02	U.S. Postal Service	CA	7/27/2016	Electronic	Government/Military	Yes - Published #	6,240

According to court documents, the former employee—who had worked at the USPS Santa Ana Processing and Distribution Center as a mail processing clerk since 1989—allegedly stole at least 6,240 credit cards from undelivered mail between Oct. 6, 2014, and Oct. 6, 2015, while working at the facility.

Attribution 1 Publication: databreaches.net Author:
Article Title: Postal employee charged with theft of thousands of credit cards
Article URL: <https://www.databreaches.net/postal-employee-charged-with-theft-of-thousands-of-credit-cards/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160722-02	College Hill Health Center	WY	7/19/2016	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Wyoming Board of Medicine Executive Director Kevin Bohnenblust said he received a call concerning the documents on Friday. The documents appear to have been found by an unnamed person who looked through the dumpster on the College Hill Health Center premises and saw what looked like official patient documents. This person then contacted a lawyer who then contacted the Board of Medicine, Bohnenblust said.

Attribution 1 Publication: wyomingbusinessreport.com Author:
Article Title: State officials investigate medical office documents
Article URL: <http://wyomingbusinessreport.com/state-officials-investigate-medical-office-documents/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160722-01	Sunbury Plaza Dental	OH	7/22/2016	Paper Data	Medical/Healthcare	Yes - Published #	7,784

We were not aware of any breach until being notified by law enforcement. Law enforcement informed us that the individuals who committed this crime gained access to the secured storage unit and did remove some of the patient records. However, the majority of the patient records in storage were not removed from the storage unit.

Attribution 1 Publication: [databreaches.net / hhs.gov / SPD websit](http://databreaches.net) Author:
Article Title: Sunbury Plaza Dental notifies patients after stored records were burglarized
Article URL: <http://www.sunburyplazadental.com/downloads/PUBLIC%20NOTICE.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 115 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-17	USA Field Hockey	CO	7/14/2016	Electronic	Business	Yes - Unknown #	Unknown

USAFH determined on June 16, 2016, that it had been the victim of a potential computer hacker intrusion. Through the investigation that followed, USAFH has determined that an unauthorized person gained access to its servers on or about March 28, 2016, and may have obtained information stored by USAFH.

Attribution 1 Publication: NH AG's office Author:
Article Title: USA Field Hockey
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/usa-field-hockey-20160714.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-16	New Hampshire Office of Professional Licensure and Certification	NH	7/11/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

By this letter, the New Hampshire Office of Professional Licensure and Certification ("OPLC") hereby notifies the New Hampshire Department of Justice of a breach of the security of confidential personal information.

Attribution 1 Publication: NH AG's office Author:
Article Title: New Hampshire Office of Professional Licensure and Certification
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/professional-licensure-20160711.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-15	American Association for the Advancement of Science /	DC	7/11/2016	Electronic	Business	Yes - Unknown #	Unknown

On behalf of the American Association for the Advancement of Science ("AAAS"), I am writing to inform you that one of our vendors, Comnet Marketing Group, Inc. ("Comnet"), recently experienced a data security incident that may have involved the personal information of eight (8) of our members in New Hampshire.

Attribution 1 Publication: NH AG's office Author:
Article Title: American Association for the Advancement of Science / Comnet Marketing Group
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/comnet-marketing-20160711.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-14	Health Incent, LLC	TN	7/11/2016	Electronic	Medical/Healthcare	Yes - Published #	1,100

Health Incent, the covered entity (CE), discovered on June 8, 2016 that a patient database containing electronic protected health information (ePHI) was available on the internet through web searches. The breach affected 1,100 individuals and the types of ePHI involved in the breach included patient names, dates of birth, email addresses, and mailing addresses. The CE provided timely breach notification to HHS, affected individuals, and the media.

Attribution 1 Publication: hhs.gov Author:
Article Title: Health Incent, LLC
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-13	Lasair Aesthetic Health, P.C.	CO	7/11/2016	Electronic	Medical/Healthcare	Yes - Published #	1,835

On May 12, 2016, we discovered that one of our former managers, after resigning, took patient identifying information by forwarding certain documents including patient lists to her personal email account. This acquisition of our patients' protected health information (PHI) was a violation of Lasair's policies and of the federal Health Insurance Portability and Accountability Act (HIPAA). Lasair has learned through its investigation that on May 11, 2016, the former employee secretly used her work email account through her mobile phone to forward to her personal email address certain documents and lists containing patient PHI.

Attribution 1 Publication: hhs.gov / Lasair website Author:
Article Title: Lasair Aesthetic Health, P.C.
Article URL: <http://lasair.com/notice-of-privacy-incident/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 116 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-11	Montana Department of Public Health and Human	MT	7/14/2016	Electronic	Government/Military	Yes - Published #	185

Montana health officials have fired two employees for providing the Social Security numbers and other personal information of 185 childcare providers to three state legislators.

The Associated Press obtained copies of letters mailed to the Republican lawmakers from Department of Public Health and Human Services director Richard Opper asking them to destroy the information and provide a list of other sensitive information given to them by the former state workers last fall.

Attribution 1 Publication: [databreaches.net / MT AG's office](#) Author:
Article Title: [State health employees fired after giving data to lawmakers](#)
Article URL: <https://dojmt.gov/wp-content/uploads/Department-of-Public-Health-and-Human-Services.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-10	Retirement Systems of Alabama	AL	7/12/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

A Mobile woman who was helping her parents with their state health insurance coverage saw names, dependent's names, dates of birth and Social Security numbers of other insurance program members on the system's website.

Attribution 1 Publication: [hipaajournal.com](#) Author:
Article Title: [PHI EXPOSED DUE TO RETIREMENT SYSTEMS OF ALABAMA WEBSITE ERROR](#)
Article URL: <http://www.hipaajournal.com/phi-exposed-retirement-systems-of-alabama-website-error-3506/>

Attribution 2 Publication: [databreaches.net / al.com](#) Author:
Article Title: [Alabama website breach revealed personal data of some state retirees](#)
Article URL: http://www.al.com/news/index.ssf/2016/07/personal_identity_data_for_som.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-09	Providence Medical Group - Gateway Clinics	OR	7/18/2016	Electronic	Medical/Healthcare	Yes - Published #	5,978

An internal audit in May revealed a former employee may have inappropriately accessed the medical records of 5,400 patients at Providence Health & Services in Oregon, reports KGW. The employee was based in Portland, and the audit indicated the employee accessed health records between July 2012 and April 2016. Potentially compromised information includes demographic and medical treatment information. The report also indicates the employee may have viewed insurance information and Social Security numbers.

Attribution 1 Publication: [beckershospitalreview.com](#) Author:
Article Title: [Providence notifies 5,400 patients of insider breach](#)
Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/providence-notifies-5-400-patients-of-inside>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-08	San Antonio Shoemakers (SAS)	TX	7/18/2016	Electronic	Business	Yes - Published #	50,000

We recently became aware of a computer intrusion that affected checkout systems at a number of San Antonio Shoemakers stores located in the United States. Promptly after discovering the issue, we engaged outside cybersecurity experts to conduct an extensive investigation. We have been working closely with law enforcement authorities and coordinating our efforts with the payment card organizations to determine the facts. (Consumers affected per IN AG's office)

Attribution 1 Publication: [VT AG's office / IN AG's office](#) Author:
Article Title: [San Antonio Shoemakers \(SAS\)](#)
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/San%20Antonio%20Shoemakers%20SBN%20to%20Co

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 117 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-07	IAP - Ingenuity and Purpose	FL	7/14/2016	Electronic	Business	Yes - Published #	4,272

On June 14, 2016, we identified that personal information was stored on a specific system affected by this incident that belonged to Readiness Management Support (RMS), IAP's wholly-owned subsidiary. The information disclosed may have included, among other items, your name, address, Social Security number, date of birth, passport information, bank account information, medical information, driver's license, and/or other government issued I D. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / IN AG's office Author:
Article Title: IAP - Ingenuity and Purpose
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/IAP%20Worldwide%20Services_%20Inc%20SBN%20to

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-06	North Palm Motors	FL	7/14/2016	Electronic	Business	Yes - Published #	22,961

On February 10, 2016, various former employees of Napleton's Car Rental Center unexpectedly quit their jobs without notice. Based upon our preliminary investigation, it appears that the breach of security involved these and other former employees and may have begun during late June 2015 and may have continued to March 9, 2016. Through the initial course of discovery and the ongoing investigation, we have recently discovered a number of additional affected parties who have had their customer information taken from Napleton's Car Rental Center without authorization, and therefore are sending this notice. This customer information includes customer names, addresses, e-mail addresses, telephone numbers, date of birth, and driver's license numbers.(Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / IN AG's Author:
Article Title: North Palm Motors
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/North%20Palm%20Motors_%20LLC%20SBN%20to%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-05	Matador Recordings dba Madador Direct	NY	7/15/2016	Electronic	Business	Yes - Unknown #	Unknown

On May 4, 2016 we were advised by our third-party website developer that it had identified and removed suspicious files from the e-commerce websites of the record labels for which Matador Direct is the distributor.

Attribution 1 Publication: CA AG's office Author:
Article Title: Matador Recordings dba Madador Direct
Article URL: https://oag.ca.gov/system/files/CA_Redacted_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-04	Opes Advisors	CA	5/26/2016	Electronic	Business	Yes - Unknown #	Unknown

On or about May 26, 2016, email login credentials were compromised allowing an outside party to gain access to one specific account. Although we are still investigating the incident, the email may have contained your private information so we wanted to let you know about this incident right away.

Attribution 1 Publication: CA AG's office / MD AG's office Author:
Article Title: Opes Advisors
Article URL: https://oag.ca.gov/system/files/Adult%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-03	Project Management Institute / Comnet Marketing Group	PA	4/24/2016	Electronic	Business	Yes - Published #	9,100

PMI was informed on June 14, 2016, that one of its vendors, Comnet Marketing Group, Inc. ("Comnet"), had been the victim of an intrusion of its computer systems. An unauthorized user gained administrative access to Comnet's systems on April 23-24, 2016, and issued commands to delete all the data housed on Comnet's servers. That data may have included certain PMI customer credit card information that Comnet had collected on behalf of PMI. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: Project Management Institute / Comnet Marketing Group
Article URL: https://oag.ca.gov/system/files/Standard%20Notice%20%284%29_1.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 118 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-02	Kaiser Permanente Northern California	CA	5/19/2016	Electronic	Medical/Healthcare	Yes - Published #	1,136

The preliminary investigation has determined that two Kaiser Permanente employees stole equipment and machines from several Kaiser Permanente sites and stored them in an offsite storage unit. When the stolen items were returned, each was examined and some of the ultrasound machines were found to contain PHI.

Attribution 1 Publication: CA AG's office Author:
Article Title: Kaiser Permanente Northern California
Article URL: <https://oag.ca.gov/system/files/Member%20Notification%20letter%20for%20ClinTech%20theft%207.12.16%20-%20gene>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160719-01	KUSC / University of Southern California / Comnet	CA	7/7/2016	Electronic	Educational	Yes - Unknown #	Unknown

KUSC recently learned that one of its contractors, Comnet Marketing Group ("Cornnet"), was affected by ransomware malware, which ultimately resulted in deletion of its storage system that housed customer credit card information. KUSC engaged Cornnet to assist with performing certain telemarketing activities, and in the course of those activities, Comnet obtained credit card information from a relatively small number of KUSC donors.

Attribution 1 Publication: Author:
Article Title: KUSC / University of Southern California
Article URL: https://oag.ca.gov/system/files/notification%20letter%20%5BFINAL%5D_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160712-09	Arkansas Spine and Pain / Bizmatics	AR	7/12/2016	Electronic	Medical/Healthcare	Yes - Published #	17,100

We have been notified by our electronic medical record vendor, Bizmatics, that cyber intruders may have installed malware on their system. Bizmatics learned of the intrusion in late 2015, however, we were notified on May 12, 2016 that our patient records were located on one of the Bizmatics servers that were affected.

Attribution 1 Publication: Databreaches.net / company website / h Author:
Article Title: Bizmatics Security Breach
Article URL: <http://arkansasaspineandpain.com/bizmatics-security-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160712-08	My Pediatrician, PA / Bizmatics	FL	6/1/2016	Electronic	Medical/Healthcare	Yes - Published #	2,500

A hacker gained access to the protected health information (PHI) for 2,385 of the covered entity's (CE) patients. The CE's business associate (BA), Bizmatics, Inc., informed the CE, My Pediatrician, PA, about this incident. The CE provided breach notification to HHS, affected individuals, and the media. The CE also created a website with information about the breach and posted substitute notification about the breach. To mitigate harm, the CE sent notice of the breach to Equifax, Transunion, and Experian and provided affected individuals with instructions for registering a fraud alert with a credit reporting agency and instructions on how to obtain a free annual credit report.

Attribution 1 Publication: hhs.gov Author:
Article Title: My Pediatrician, PA
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf?jsessionid=3975E32FC15E58D3DF65A24B4CA5522C.ajp13w

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160712-07	North Ottawa Medical Group / Bizmatics	MI	6/9/2016	Electronic	Medical/Healthcare	Yes - Published #	22,000

The Michigan-based medical group was notified by Bizmatics that servers containing patient information were accessed by an unauthorized user. Although the vendor could not confirm if North Ottawa Medical Group's patient files were involved in the incident.

Attribution 1 Publication: hhs.gov / healthitsecurity.com Author:
Article Title: North Ottawa Medical Group / Bizmatics
Article URL: <http://healthitsecurity.com/news/bizmatics-healthcare-data-breach-affects-another-22k-patients>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160712-06	Laser & Dermatologic Surgery Center	MO	6/14/2016	Electronic	Medical/Healthcare	Yes - Published #	31,000

On March 21, 2016., after a review of access logs was conducted, it was also discovered that an unauthorized individual had gained access to the healthcare provider's network. The first intrusion was determined to have taken place on March 1, 2016.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](http://hhs.gov/hipaajournal.com) Author:
Article Title: DETAILS EMERGE ON LASER DERMATOLOGIC SURGERY CENTER DATA BREACH
Article URL: <http://www.hipaajournal.com/details-emerge-on-laser-dermatologic-surgery-center-data-breach-3525/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160712-05	Midland Women's Clinic / Mario M. Gross, M.D.	TX	6/17/2016	Paper Data	Medical/Healthcare	Yes - Published #	717

On April 26, 2016, Clinic representatives discovered that Mario M. Gross, M.D., a physician who was last employed with the Clinic in 2006, had left patient information at his private residence, causing the information to be accessible to certain members of the public for a limited period of time. Upon the discovery of the patient records, the records were promptly secured, and an internal investigation was initiated to determine the specific patients who were affected and the personal information that was contained in those records.

Attribution 1 Publication: [hhs.gov / clinic website](http://hhs.gov/clinic-website) Author:
Article Title: Midland Women's Clinic
Article URL: <https://www.databreaches.net/physician-took-work-home-and-there-it-stayed-after-his-employment-terminated/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160712-04	Uncommon Care, P.A. / Bizmatics	NC	6/21/2016	Electronic	Medical/Healthcare	Yes - Published #	13,674

Uncommon Care, PA is committed to protecting patient information. This commitment includes notifying patients if there is a possibility that someone may have obtained access to their information. Uncommon Care uses a company called Bizmatics, Inc. to electronically store the medical information of our patients. We were informed by Bizmatics that in 2015 there had been an unauthorized access to certain electronic medical records in their custody. Bizmatics, however, could not determine that the records of Uncommon Care patients were affected.

Attribution 1 Publication: [hhs.gov / databreaches.net](http://hhs.gov/databreaches.net) Author:
Article Title: Uncommon Care, PA notifies almost 14,000 patients of Bizmatics breach
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160712-02	Ambulatory Surgery Center at St. Mary	PA	7/12/2016	Electronic	Medical/Healthcare	Yes - Published #	13,000

In letters sent to patients last week, the center, which provides outpatient surgical and diagnostic procedures, explained that staff members discovered the breach June 1 when they noticed encrypted files on an internal network. The center is owned by St. Mary Medical Center and local physicians, and is in the St. Clare Medical Building on the hospital's main Middletown campus.

Attribution 1 Publication: databreaches.net Author:
Article Title: Ransomware attacks info of 13K patients at Ambulatory Surgery Center at St. Mary
Article URL: <https://www.databreaches.net/pa-ransomware-attacks-info-of-13k-patients-at-ambulatory-surgery-center-at-st-mary/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160712-01	Pennsylvania Department of Revenue	PA	7/12/2016	Electronic	Government/Military	Yes - Published #	865

In late June, four department auditors were in San Francisco, California to conduct a routine audit. At approximately 6:00 PM thieves smashed the windows of several parked vehicles, including the auditors' locked rental vehicle, stealing four laptop computers. The employees immediately began working with law enforcement and notified the department. The stolen laptops have not been recovered.

Attribution 1 Publication: databreaches.net Author:
Article Title: Laptop theft puts personal information of hundreds of Pennsylvania taxpayers at risk
Article URL: <https://www.databreaches.net/laptop-theft-puts-personal-information-of-hundreds-of-pennsylvania-taxpayers-at-risk/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 120 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160711-05	TD Bank	NJ	7/5/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently learned that one of our employees improperly obtained some of our customers' personal information. The personal information they obtained may have included their name, address, social security number, date of birth, account numbers and balances.

Attribution 1 Publication: NH AG's office Author:
 Article Title: TD Bank
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/td-bank-20160628.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160711-04	Midland Memorial Hospital / Mario M. Gross, M.D.	TX	7/8/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,468

On April 8, 2016, the Midland, Texas-based hospital was alerted to a privacy breach that exposed patients' names, addresses, dates of birth, medical diagnoses, medications, medical procedures, physician's notes, medical record unit numbers, medical account numbers, and health information. In some cases, patients also had their Social Security numbers exposed.

Attribution 1 Publication: hipaajournal.com Author:
 Article Title: MIDLAND MEMORIAL HOSPITAL ANNOUNCES POTENTIAL PHI BREACH
 Article URL: <http://www.hipaajournal.com/midland-memorial-hospital-announces-potential-phi-breach-3496/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160711-03	North Carolina State University	NC	7/11/2016	Electronic	Educational	Yes - Published #	38,976

A cyber crook used a phishing scam to break into a North Carolina State University email account containing personally identifiable information. What type of information? Names, home address from 2013, student ID numbers, and social security numbers were all compromised. (Consumers affected per IN AG's office)

Attribution 1 Publication: scmagazine.com / VT AG's office / MD Author:
 Article Title: NC State breach affects 38,000
 Article URL: <http://www.scmagazine.com/nc-state-breach-affects-38000/article/508601/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160711-02	PruittHealth Hospice - Beaufort	GA	6/30/2016	Electronic	Medical/Healthcare	Yes - Published #	1,437

In a separate healthcare data security incident, thieves had broken into the PruittHealth Hospice-Beaufort office on April 11 by breaking the glass of a side window. The perpetrators also managed to break into patient file cabinets that contained paper medical records. While the perpetrators reportedly did not disturb any patient files, individuals may still have had their PHI disclosed in both events, including names, addresses, Social Security numbers, dates of birth, dates of services, locations of service, and other clinical information.

Attribution 1 Publication: healthitsecurity.com Author:
 Article Title: Healthcare System Break-Ins Result in Potential PHI Breaches
 Article URL: <http://healthitsecurity.com/news/healthcare-system-break-ins-result-in-potential-phi-breaches>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160711-01	California Department of Corrections and	CA	6/30/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

We are writing to you because of a security incident that occurred on May 2, 2016 at the California Health Care Facility. An employee inadvertently e-mailed a document containing your personal information to the wrong person.

Attribution 1 Publication: CA AG's office Author:
 Article Title: CDCR - California Health Care Facility
 Article URL: https://oag.ca.gov/system/files/CHCF%20Privacy%20Breach%20Letter_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 121 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160708-01	Omni Hotels and Resorts	TX	7/8/2016	Electronic	Business	Yes - Published #	50,000

On May 30, 2016, we discovered we were the victim of malware attacks on our network affecting specific point of sale systems on-site at some Omni properties. The malware was designed to collect certain payment card information, including cardholder name, credit/debit card number, security code and expiration date. We have no indication that reservation or Select Guest membership systems were affected.

Attribution 1 Publication: pymnts.com Author:
 Article Title: SECURITY & FRAUDPYMNTS Daily Data Dive: Omni Breach
 Article URL: <http://www.pymnts.com/news/security-and-risk/2016/omni-hotels-breach-data/>

Attribution 2 Publication: CA AG's office / SC AG's office Author:
 Article Title: Omni Hotels and Resorts
 Article URL: https://oag.ca.gov/system/files/NoticeofDataBreach070816_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160705-07	Allergy, Asthma & Immunology of the Rockies	CO	6/17/2016	Electronic	Medical/Healthcare	Yes - Published #	6,851

Colorado-based Allergy, Asthma & Immunology of the Rockies, P.C. (AAIR) reported that it found evidence of ransomware on its computer systems on May 16. The disturbance was first noticed when there was some difficulty in accessing documents, AAIR attorney Kari Hershey told The Post Independent. While AAIR did not specify what type of information may have been affected, it was reported that their system contained PHI, including test results and Social Security numbers. However, AAIR immediately shut the server down upon realizing the potential breach of information and contacted a forensic IT company.

Attribution 1 Publication: hhs.gov / healthitsecurity.com Author:
 Article Title: CO Clinic Healthcare Ransomware Case Affects 6,800 Patients
 Article URL: <http://healthitsecurity.com/news/co-clinic-healthcare-ransomware-case-affects-6800-patients>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160705-06	Office of Linda J. White, DDS, PC	VA	6/27/2016	Electronic	Medical/Healthcare	Yes - Published #	2,000

On June 27, 2016, the covered entity (CE), Dr. Linda White, reported that an external hard drive device containing a backup of the dental practice's computer server was not returned for proper destruction by an employee. Approximately 2,000 individuals were affected by the breach and the types of protected health information (PHI) stolen included patients' names, dates of births, social security numbers, and limited medical information. The CE provided breach notification to HHS, affected individuals, and the media.

Attribution 1 Publication: hhs.gov Author:
 Article Title: Office of Linda J. White, DDS, PC
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160705-05	Capella University	MN	6/29/2016	Electronic	Educational	Yes - Unknown #	Unknown

On June 17, 2016 we discovered that, on June 17, 2016, a Capella employee inadvertently e-mailed XXXX your and information to a third-party, in violation of Capella policy. Upon investigation, Capella determined that the XXX also contained the same information for another adult and four dependent children.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Capella University
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Capella%20University%20SBN%20to%20Consumer%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160705-04	KontrolFreek, LLC	GA	6/30/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently became aware that an unauthorized third party accessed the KontrolFreek servers and acquired certain payment card information of some of our customers. Promptly after learning of the issue, we took steps to secure our website and determine the nature and scope of the issue. In addition, we retained a data security expert to conduct a forensic investigation. Based on the investigation, we believe the issue occurred between October 21, 2015 and April 7, 2016. The affected information may have included your name, address, payment card number and security code.

Attribution 1 Publication: CA AG's office Author:
Article Title: KontrolFreek, LLC
Article URL: https://oag.ca.gov/system/files/California%20Individual%20Notification%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160705-03	Kool Kids Model & Talent Management	CA	2/16/2016	Electronic	Business	Yes - Unknown #	Unknown

APPLE Store referred us to ACS Computer Services to remove the hard drive from our MacBook Pro prior to a repair service. While removing the hard drive and transferring it to an external hard drive case ACS COMPUTER SERVICES allegedly misplaced the MacBook Pro hard drive. Unfortunately the hard drive includes personal identifiable information for all current and former Kool Kids clients, talent as well as family members and applicants, including names, social security numbers, addresses, bank account numbers, and payroll records.

Attribution 1 Publication: CA AG's office Author:
Article Title: Kool Kids Model & Talent Management
Article URL: https://oag.ca.gov/system/files/Security%20Breach%20Filed_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160705-02	Massachusetts General Hospital / Patterson Dental	MA	6/30/2016	Electronic	Medical/Healthcare	Yes - Published #	4,293

Massachusetts General Hospital (MGH) has announced that some patients of its dental group had their protected health information exposed earlier this year. The security breach occurred at one of the healthcare provider's business associates, Patterson Dental Supply Inc., (PDSI). Massachusetts General Hospital

Attribution 1 Publication: hipaajournal.com / VT AG's office / NH A Author:
Article Title: MASSACHUSETTS GENERAL HOSPITAL REPORTS PHI INCIDENT
Article URL: <http://www.hipaajournal.com/massachusetts-general-hospital-reports-phi-incident-3489/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160705-01	Planned Parenthood of the Heartland	IA	7/5/2016	Paper Data	Medical/Healthcare	Yes - Published #	2,506

On July 1, 2016, Planned Parenthood of the Heartland announced that the protected health information (PHI) of certain patients of its Dubuque health center in Iowa may have been accessed by unauthorized individuals. Patient files contained full names, mailing addresses, dates of birth, health insurance information, Social Security numbers, medical record numbers, lab test results, medical diagnoses, and treatment information.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: POTENTIAL PRIVACY BREACH AT PLANNED PARENTHOOD DUBUQUE HEALTH CENTER
Article URL: <http://www.hipaajournal.com/potential-privacy-breach-planned-parenthood-dubuque-health-center-3492/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160628-06	Holley Central School District	NY	6/23/2016	Electronic	Educational	Yes - Unknown #	Unknown

According to cloud security company BatBlue Networks, a secretary at the New York-based school district discovered an attack from back in April 2016. In the attack, hackers stole information on over 150 employees and contractors, in addition to thousands more who worked for the district any time before 2004.

Attribution 1 Publication: siliconangle.com Author: Robert Pleasant
Article Title: New York school district suffers a hack and data breach
Article URL: <http://siliconangle.com/blog/2016/06/23/new-york-school-district-suffers-a-hack-and-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160628-05	TD Bank	NJ	6/13/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently experienced a privacy issue but we're making things right. We recently learned that one of our employees improperly obtained some of your personal information between January 14th, 2016 and May 9th, 2016. The personal information they obtained may have included your name, address, social security number, date of birth and account numbers and balances.

Attribution 1 Publication: NH AG's office Author:
Article Title: TD Bank
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/td-bank-20160613.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160628-04	Benchmark Senior Living	MA	6/22/2016	Electronic	Business	Yes - Published #	218

Please be advised that on June 14, 2016, Benchmark Senior Living ("Company") discovered a potential data breach when it learned of an intrusion into the company's systems affecting payroll data. The personal information potentially included in the incident included name, address, social security number and bank account information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Benchmark Senior Living
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/benchmark-20160622.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160628-03	Riverside Health System	VA	6/10/2016	Paper Data	Medical/Healthcare	Yes - Published #	578

An employee authorized to work from home failed to return paper records to the physician practice. Her ex-husband discovered the records and returned them to the physician practice. The breach included the protected health information (PHI) of 578 individuals. The PHI involved in the breach included demographic information, dates of birth, social security numbers, medical records numbers, and clinical information.

Attribution 1 Publication: hhs.gov Author:
Article Title: Riverside Health System
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160628-02	Gamesa Wind US, LLC	PA	6/27/2016	Electronic	Business	Yes - Unknown #	Unknown

On Friday June 17, 2016, we learned that earlier on the same day, an employee of the Company, while traveling on business, received a spoofed "phishing" email message constructed to appear as if it came from Ignacio Martin, Executive Chairman of the Company's global parent company Gamesa Corporacion Tecnologica, S.A. This employee, thinking they were responding to a legitimate request from the Executive Chairman for US payroll and tax records, provided to the unknown third party behind the phishing email the Company's 2015 W-2 forms, including your 2015 W-2.

Attribution 1 Publication: VT AG's office Author:
Article Title: Gamesa Wind US, LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Games%20Wind%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160628-01	SP+ Municipal Services	MD	6/25/2016	Electronic	Business	Yes - Unknown #	Unknown

On June 11, the city's parking contractor, SP+ Municipal Services, found malware on servers that can take credit and debit card information of from people using the Noah Hillman, Gott's Court and Knighton garages.

Attribution 1 Publication: capitalgazette.com Author:
Article Title: Annapolis parking garages accepting credit cards again
Article URL: <http://www.capitalgazette.com/news/annapolis/ph-ac-cn-data-breach-update-0625-20160624-story.html>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 124 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160627-03	Sageworks, Inc.	NC	6/22/2016	Electronic	Business	Yes - Unknown #	Unknown

In January of 2015, we discovered that retained personal information about certain Sageworks, Inc. ("Sageworks") employees after his employment terminated in November of 2014. Personal information about you was included in the documents he retained.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: Sageworks, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Sageworks%20Inc%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160627-02	Hard Rock Hotel & Casino Las Vegas	NV	6/27/2016	Electronic	Business	Yes - Unknown #	Unknown

On May 13, 2016, the investigation identified signs of unauthorized access to the resort's payment card environment. Further investigation revealed the presence of card scraping malware that was designed to target payment card data as the data was routed through the resort's payment card system.

Attribution 1 Publication: CA AG's office / SC AG's office Author:
Article Title: Hard Rock Hotel & Casino Las Vegas
Article URL: https://oag.ca.gov/system/files/Hard%20Rock%20-%20Regulatory%20Packet%20%28CA%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160627-01	Dignity Health / Mercy Medical Center Redding	CA	6/13/2016	Electronic	Medical/Healthcare	Yes - Published #	520

On June 6, 2016., Dignity Health was informed by naviHealth that an individual had gained employment under false pretenses. The individual was employed by naviHealth as a case worker between June 2015 and May 2016. The case worker was provided with access to the protected health information (PHI) of 520 patients during the time of employment in order to complete work duties. All of the patients had previously received medical services at Mercy Medical Center Redding.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Dignity Health / Mercy Medical Center Redding
Article URL: <http://www.hipaajournal.com/case-manager-duped-navihealth-dignity-health-alerts-patients-to-privacy-breach-3484/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160624-02	Texas Health and Human Resources Commission	TX	6/14/2016	Paper Data	Government/Military	Yes - Published #	600

Between April 19, 2016 and May 10, 2016, Iron Mountain, a business associate (BA) of the covered entity (CE), Texas Health and Human Services Commission, was unable to locate sixteen cartons of records containing protected health information (PHI). The types of PHI involved in the breach included the names, addresses, social security numbers, social security claim numbers, dates of birth, medical record numbers, Medicaid/individual numbers, case numbers, and bank account numbers for over 500 individuals. Additionally, the CE initiated a change to its procedure for reconciling file inventories and verifying file box destruction. OCR obtained assurances that the CE implemented the corrective actions noted above.

Attribution 1 Publication: hhs.gov Author:
Article Title: Texas Health and Human Resources Commission
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160624-01	Saints Mary and Elizabeth Hospital	KY	6/10/2016	Electronic	Medical/Healthcare	Yes - Published #	1,682

Saints Mary and Elizabeth Hospital KY Healthcare Provider 1682 06/10/2016 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Saints Mary and Elizabeth Hospital
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 125 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160621-05	Washington Redskins	DC	6/1/2016	Electronic	Business	Yes - Unknown #	Unknown

Washington Redskins officials said Wednesday they're working with the NFL and NFL Players Association to notify thousands of players whose medical records may have been breached after a backpack containing electronic and paper files was stolen from the car of a team athletic trainer April 15 in Indianapolis. According to Deadspin, which was first to report the story, the thief took a backpack that contained "a cache of electronic and paper medical records" of thousands of athletes.

Attribution 1 Publication: WashingtonPost.com Author: Liz Clarke
Article Title: Redskins employee's laptop stolen; NFL trying to determine extent of the breach
Article URL: <https://www.washingtonpost.com/sports/redskins/redskins-employees-laptop-stolen-but-medical-records-not-feared-c>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160621-04	State Farm Mutual Automobile Insurance	IL	6/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On January 21, 2016, State Farm opened an investigation related to employees of a State Farm independent contractor agent in Chino Hills, CA. The investigation determined there was misappropriation of customer funds as well as misuse of customer financial cards to make payments and/or replace customer payments that were either diverted or not correctly applied to customers' accounts. At this time, our investigation has identified misappropriation of customer funds, misuse of some customer financial cards, and accessing and changing some customers' contact information. In addition, in some instances information was used to add additional insurance coverage without the policyholders' knowledge and consent.

Attribution 1 Publication: CA AG's office Author:
Article Title: State Farm Mutual Automobile Insurance Company
Article URL: http://oag.ca.gov/system/files/Breach%20Notification%20ISRR%2005116037-2016%20%20Letter%201A_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160621-03	Santa Rosa Consulting	CA	6/13/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

The company was the target of a third-party fraudulent phishing scheme. On May 8, 2016, W2 information of our employees, intended for company officers entitled to receive such information, was unknowingly diverted to an unidentified third-party. This information includes names, addresses and Social Security numbers.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Santa Rosa Consulting
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/santa-rosa-consulting-20160613.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160621-02	Massachusetts Eye and Ear Infirmary, Inc.	MA	6/16/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Attribution 1 Publication: NH AG's office Author:
Article Title: Massachusetts Eye and Ear Infirmary, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/mass-eye-ear-20160616.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160621-01	Crane Payment Innovations, Inc.	PA	6/8/2016	Electronic	Business	Yes - Unknown #	Unknown

Earlier today, a CPI employee responded to an e-mail that appeared to come from me, requesting a copy of your 2015 W-2 wage statement, which included your Social Security number, wage information and home address. Unfortunately, we learned later that day that the e-mail was not, in fact, from me, but rather was part of a fraudulent scheme, and your personal information was sent to an unknown individual.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Crane Payment Innovations, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/crane-20160608.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 126 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160620-09	GoToMyPC	CA	6/20/2016	Electronic	Business	Yes - Unknown #	Unknown

GoToMyPC, a service that helps people access and control their computers remotely over the Internet, is forcing all users to change their passwords, citing a spike in attacks that target people who re-use passwords across multiple sites.

Attribution 1 Publication: [krebsonsecurity.com](#) Author:
Article Title: Citing Attack, GoToMyPC Resets All Passwords
Article URL: <http://krebsonsecurity.com/2016/06/citing-attack-gotomypc-resets-all-passwords/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160620-08	Vein Doctor / Bizmatics	MO	6/3/2016	Electronic	Medical/Healthcare	Yes - Published #	3,000

A breach notice has not appeared on the healthcare provider's website at the time of posting, and it is unclear how much protected health information was exposed in the cyberattack. However, the breach does appear to be linked to Bizmatics. The Vein Doctor uses the Prognosis EMR tool developed and maintained by Bizmatics. Other healthcare providers impacted by the Bizmatics breach also used the Prognosis too

Attribution 1 Publication: [hhs.gov / hipaajournal.com](#) Author:
Article Title: Vein Doctor / Bizmatics
Article URL: <http://www.hipaajournal.com/bizmatics-data-breach-victim-count-rises-almost-177000-3483/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160620-07	Grace Primary Care, PC / Bizmatics	TN	6/7/2016	Electronic	Medical/Healthcare	Yes - Published #	6,853

Grace Primary Care P.C., also reported a data breach to the OCR which was similarly caused by the hacking of a network server. The breach report, submitted to the OCR on June 7, 2016., indicates the PHI of 6,853 patients was potentially exposed. Grace Primary Care also uses the Prognosis tool for its patient portal, and is another likely victim of the Bizmatics data breach.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](#) Author:
Article Title: Grace Primary Care, PC / Bizmatics
Article URL: <http://www.hipaajournal.com/bizmatics-data-breach-victim-count-rises-almost-177000-3483/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160620-06	TieMart, Inc.	IL	6/16/2016	Electronic	Business	Yes - Published #	927

Between 5/4/2016 and 5/19/2016 hackers placed malware code on our tiemart.com website. On 6/3 we were able to determine that the code was electronically sending names, addresses and credit card information to an unknown third party location.

Attribution 1 Publication: [NH AG's office / MD AG's office](#) Author:
Article Title: TieMart, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/tiemart-20160613.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160620-05	Sandler & Travis Trade Advisory Services, LLC	DC	6/13/2016	Electronic	Business	Yes - Unknown #	Unknown

Specifically, on April 14, 2016, an STTAS employee received a request for all 2015 employees' W-2 information. This information was provided prior to the discovery that the request had been made from a fraudulent account by an individual purporting to be an STTAS executive. When the spoofed email returned on April 19, 2016, STTAS confirmed that the initial email was a spear phishing attack.

Attribution 1 Publication: [NH AG's office / MD AG's office](#) Author:
Article Title: Sandler & Travis Trade Advisory Services, LLC
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/sandler-travis-20160613.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160620-04	Wal-Mart	AR	6/16/2016	Electronic	Medical/Healthcare	Yes - Published #	27,393

Recently, we learned that the company that processes our patient refund checks experienced a printing error. This error caused incorrect information to be printed on the letters that accompanied the refund checks sent to customers. As a result, the mailing a customer received may have included another individual's information, limited to: (1) name, (2) a pharmacy prescription number or an optical order number, (3) the order date, and (4) a refund amount. The city and state of the Walmart or Sam's Club visited also was included.

Attribution 1 Publication: [databreaches.net / hhs.gov](http://databreaches.net/hhs.gov) Author:
Article Title: Walmart vendor error exposed limited patient information
Article URL: <https://www.databreaches.net/wal-mart-vendor-error-exposed-limited-patient-information/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160620-03	ENT and Allergy Center / BizMatics	AR	6/17/2016	Electronic	Medical/Healthcare	Yes - Published #	16,200

In a statement dated May 31, that is linked from their web site, Stephen Cashman, M.D., states that the practice was initially notified of the incident in January, 2016. But, "At that time, Bizmatics could not conclude that our patient records were among those that were accessed and had no reason to believe that the data that was compromised had been published or shared in any public manner."

Attribution 1 Publication: databreaches.net Author:
Article Title: ENT and Allergy Center of Arkansas notifying patients of Bizmatics security incident
Article URL: <https://www.databreaches.net/ent-and-allergy-center-of-arkansas-notifying-patients-of-bizmatics-security-incident/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160620-02	Hamilton General Hospital	TX	6/17/2016	Electronic	Medical/Healthcare	Yes - Published #	397

An employee snooped into the medical records of 397 patients at Hamilton General Hospital. The staff member was fired after an investigation by Hamilton Health Sciences concluded the privacy of emergency room patients was breached from June 2015 to May 2016.

Attribution 1 Publication: [thespec.com / databreaches.net](http://thespec.com/databreaches.net) Author: Joanna Frketich
Article Title: 397 medical records snooped at Hamilton General Hospital
Article URL: <http://www.thespec.com/news-story/6729448-397-medical-records-snooped-at-hamilton-general-hospital/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160620-01	Multi-Color Corporation	OH	5/15/2016	Electronic	Business	Yes - Published #	4,602

On May 16,2016, the law firm informed Multi-Color that someone broke into the law firm's law offices on either May 14 or May 15 and stole several items, including the hard drive containing Multi-Color's data and the password.

Attribution 1 Publication: CA AG's office / MD AG's office / IN AG' Author:
Article Title: Multi-Color Corporation
Article URL: https://oag.ca.gov/system/files/Final%20Notice%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160615-02	University of Connecticut - School of Engineering	CT	5/31/2016	Electronic	Educational	Yes - Unknown #	Unknown

On March 9, 2015, Information Technology (IT) staff in the School of Engineering detected that malicious software, or "malware," had been placed on a number of servers that are part of the School's technical infrastructure over a period of months, with penetration of the servers beginning as early as September 2013. As part of the complex and thorough investigation that remains underway, it has been determined that some of the files maintained on those impacted servers contained personal information, such as names, contact information, Social Security numbers, employment information, student academic information, research data and School of Engineering graduate level admissions data.

Attribution 1 Publication: CA AG's office Author:
Article Title: University of Connecticut
Article URL: https://oag.ca.gov/system/files/Sample%20Notif%20Ltr%201_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 128 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160615-01	Vermont Department of Fish and Wildlife	VT	6/15/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

While the details of the data breach have not been disclosed, The Washington Times reports that evidence suggests an unauthorized party had access to the servers from April 2015 up until January 2016. As such, personal details such as names, addresses, and license information could have been accessed during that time, and may have been or will be misused.

Attribution 1 Publication: databreaches.net Author:
Article Title: Vermont Fish and Wildlife reports license data breach
Article URL: <http://www.databreaches.net/vermont-fish-and-wildlife-reports-license-data-breach/>

Attribution 2 Publication: siliconangle.com Author: Robert Pleasant
Article Title: Bad catch: Vermont Fish and Wildlife Department suffers data breach
Article URL: <http://siliconangle.com/blog/2016/06/15/vermont-fish-and-wildlife-department-suffers-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-17	Primary Residential Mortgage	UT	5/9/2016	Electronic	Banking/Credit/Financial	Yes - Published #	2,889

We just discovered that on February 25, 2016, Primary Residential Mortgage, Inc. was the target of a "phishing" attack that resulted in the release of a copy of your 2015 W-2 form to an unknown third party. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office / MD AG' Author:
Article Title: Primary Residential Mortgage
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/primary-residential-20160609.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-16	EPTAM Plastics	NH	5/27/2016	Electronic	Business	Yes - Unknown #	Unknown

On May 18, 2016, EPTAM received an email purporting to be from its President Jeff Hollinger requesting copies of all employee Form W-2's. Unfortunately this information was provided before EPTAM discovered that the request was made from a fraudulent account by an individual using Mr. Hollinger's name.

Attribution 1 Publication: NH AG's office Author:
Article Title: EPTAM Plastics
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/eptam-plastics-20160527.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-15	Bucknell University	PA	6/7/2016	Electronic	Educational	Yes - Unknown #	Unknown

Bucknell University faculty and staff are provided with an internal electronic document storage application called Netspace. Within Netspace, certain folders are accessible to all individuals with both University login credentials and an additional level of authorization. As part of Bucknell's ongoing electronic security efforts, it deployed a tool to scan those Netspace folders in order to identify any sensitive data being stored there. On or around March 31, 2016 and April 11, 2016, Bucknell identified sensitive data elements located in a limited number of those Netspace folders

Attribution 1 Publication: NH AG's office / VT AG's office / MD AG' Author:
Article Title: Bucknell University
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/bucknell-20160603.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-14	ARIAD Pharmaceuticals	MA	5/31/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

The disclosure that occurred was the result of human error prompted by a sophisticated phishing scam. The incident did not involve any customer information or an intrusion into ARIAD's computer systems or network.

Attribution 1 Publication: NH AG's office Author:
Article Title: ARIAD Pharmaceuticals
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/ariad-pharmaceuticals-20160531.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-13	Quarles & Brady, LLP	WI	4/19/2016	Electronic	Business	Yes - Published #	1,032

Quarles & Brady, LLP WI Business Associate 1032 04/19/2016 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Quarles & Brady, LLP
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-12	Office of Allen Dell, PA	FL	6/1/2016	Electronic	Medical/Healthcare	Yes - Published #	2,500

Allen Dell, P.A .FL Business Associate 2500 06/01/2016 Hacking/IT IncidentNetwork Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Allen Dell, PA
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-11	Washington State Liquor and Cannabis Board	WA	6/7/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

The Washington State Liquor and Cannabis Board is working to notify marijuana license applicants whose personal information was accidentally distributed by the agency in response to a public records request. The data may include social security numbers, driver's license numbers, financial information, tax information and attorney-client privileged information. The LCB had redacted the documents for the records request, but a folder containing the personal information was accidentally included.

Attribution 1 Publication: databreaches.net Author:
Article Title: Washington marijuana applicants' personal info subject to data breach
Article URL: <http://www.databreaches.net/washington-marijuana-applicants-personal-info-subject-to-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-10	Town of Saugus - Lawsuit Discovery	MA	6/9/2016	Electronic	Government/Military	Yes - Published #	1,200

When attorney Elayne Alanis requested documents relating to the employment of Saugus' former Information Technology Network Administrator James Rivers, she wasn't expecting 48,960 pages. More upsetting than the overwhelming volume of documents, Alanis said, was the inclusion of 1,200 town employees' Social Security numbers, tax documents and personal banking information.

Attribution 1 Publication: saugus.wickedlocal.com Author: Jeannette Hinkle
Article Title: Saugus employees' personal information released during discovery phase of Rivers lawsuit against town
Article URL: <http://saugus.wickedlocal.com/article/20160609/NEWS/160606453/?Start=1>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-09	Virginia's State Corporation Commission	VA	6/10/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

If you sold insurance in Virginia but your license lapsed or expired between 1979 and 2004, a state agency suspects your personal information may have been stolen. Virginia's State Corporation Commission says a former contractor for the agency may have copied insurance agent files that included names, Social Security numbers or driver's licenses.

Attribution 1 Publication: databreaches.net / pilotonline.com Author:
Article Title: Virginia's State Corporation Commission
Article URL: http://pilotonline.com/business/insurance-agents-in-virginia-may-have-had-personal-data-stolen/article_c8052cf4-513f-

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 130 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-08	Nationwide Retirement Solutions	OH	6/10/2016	Electronic	Banking/Credit/Financial	Yes - Published #	457

Workers with Nationwide Retirement Solutions noticed "suspicious activity" with some 457 deferred compensation accounts for municipal employees similar to 401k accounts on June 1, a company spokesman said. These accounts are administered by Nationwide on behalf of the city, according to the city comptroller's office.

Attribution 1 Publication: nj.com / databreaches.net Author:
Article Title: Bamboozled: After Chicago retirement account breach, could NJ pensions be next?
Article URL: http://www.nj.com/business/index.ssf/2016/06/after_chicago_retirement_account_breach_could_njs.html

Attribution 2 Publication: chicagotribune.com Author: John Kass and Willia
Article Title: Officials investigate breach of retirement accounts
Article URL: <http://www.chicagotribune.com/news/local/breaking/ct-officials-investigate-breach-of-retirement-accounts-20160610-s>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-07	Sutter County Superior Courthouse	CA	6/14/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

Private personal information of potentially thousands of people was unintentionally available on public access computers in the Sutter County Superior Courthouse on Monday.

Attribution 1 Publication: databreaches.net Author:
Article Title: Courthouse data breach exposes personal information
Article URL: http://www.appeal-democrat.com/news/courthouse-data-breach-exposes-personal-information/article_80a08626-31fa-1

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-06	Vincent Vein Center Grand Junction / Bizmatics	CO	6/13/2016	Electronic	Medical/Healthcare	Yes - Published #	2,250

The breach notice submitted to OCR by the Vincent Vein Center was received on June 7, 2016, more than two months after being notified of the potential breach by Bizmatics. The OCR report shows that 2,250 patients potentially had their PHI compromised. The breach notice posted on the Vincent Vein Center website indicates the same data elements were potentially viewed or copied by the attacker, although in some cases Social Security numbers were also exposed.

Attribution 1 Publication: hipaajournal.com / databreaches.net / w Author:
Article Title: Vincent Vein Center Grand Junction / Bizmatics
Article URL: <http://vincentvein.com/website-notification/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-05	Kern County Mental Health Department	CA	6/14/2016	Paper Data	Government/Military	Yes - Published #	1,212

A single document was left behind in the offices and could potentially have been viewed by construction workers. The document was discovered by a KCMH staff member upon return to the offices. During the time that the report was left unprotected, staff members did not have access to the area. The report contained patients' full names, internal record numbers, service codes, and the unit where treatment was provided.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: KERN COUNTY MENTAL HEALTH DEPARTMENT ANNOUNCES PRIVACY BREACH
Article URL: <http://www.hipaajournal.com/kern-county-mental-health-department-announces-privacy-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-04	SD Associates, P.C.	PA	6/6/2016	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you that on April 26, 2016, SD Associates was informed by the IRS Criminal Division that data within our database concerning some of our clients was compromised. Some of that data was used to file phony electronic tax returns by criminals who sought to obtain refunds from the IRS using the stolen information.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: SD Associates, P.C.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/SD%20Associates%20PC%20SBN%20to%20Consumer

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-03	Cohen & Grieb, P.A.	FL	6/1/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 4, 2016, we learned that an unauthorized individual was able to gain access to our network through an account set up by our outside IT provider. We selected this company because they are well-regarded as one of the top local IT service providers. It appears that the unauthorized individual may have accessed certain client files while on our network between March 27, 2016 and April 4, 2016, when our IT provider disabled access for the affected account.

Attribution 1 Publication: VT AG's office / NH AG's office / MD AG' Author:
Article Title: Cohen & Grieb, P.A.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Cohen%20%20Grieb%20PA%20SBN%20to%20Consu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-02	Acer Service Corporation	TX	6/14/2016	Electronic	Business	Yes - Published #	34,500

We recently identified a security issue involving the information of certain customers who used our ecommerce site between May 12, 2015 and April 28, 2016, which resulted in unauthorized access by a third party. Based on our records, we have determined that your information may have been affected, potentially including your name, address, card number ending in [insert], expiration date and three-digit security codes. We do not collect Social Security numbers, and we have not identified evidence indicating that password or login credentials were affected.

Attribution 1 Publication: CA AG's office / OR AG's office / Scmag Author:
Article Title: Acer Service Corporation
Article URL: https://oag.ca.gov/system/files/Customer%20Notice%20Letter%20-%20California_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160614-01	Momentum for Mental Health	CA	6/9/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On June 3, 2016, Momentum was targeted by an e-mail scam called "spoofing." We discovered this incident within hours of it taking place. Nonetheless, it resulted in Momentum inadvertently making personal information from your Form W-2 available to an unknown third party.

Attribution 1 Publication: CA AG's office Author:
Article Title: Momentum for Mental Health
Article URL: https://oag.ca.gov/system/files/Crrnt%20Emply.MMH_.Data%20Breach%20Notice%20%283%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160610-01	State Farm / DAC Group	IL	6/9/2016	Electronic	Business	Yes - Published #	7,570

Cyber criminals reportedly breached the servers of digital marketing firm DAC Group and accessed 77,000 State Farm customer accounts. The attackers were able to steal information on 93,000 client accounts from the server of Toronto-based DAC Group, according to reports. At least 77,000 of those stolen accounts belong to State Farm in Bloomington, Illinois. The 93,000 stolen accounts reportedly include customers' encrypted passwords, full names, geolocation, usernames and other data. (Consumers affected per IN AG's office)

Attribution 1 Publication: batblue.com / CA AG's office / IN AG's o Author:
Article Title: Data Breach Exposes 77,000 State Farm Customers
Article URL: <http://www.batblue.com/data-breach-exposes-77000-state-farm-customers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160608-01	Concord School District	NH	6/3/2016	Electronic	Educational	Yes - Unknown #	Unknown

The Concord School District reported on June 3, 2016, that it has been hit with a "Data Security Breach" in two months ago that compromised the W-2 forms of everyone receiving payment from the school in 2015, according to a press statement. The "social engineering attack" hit the district on April 7, 2016, according to School Superintendent Terri Forsten. The district found out about the attack on June 1. Forsten sent a letter to everyone who had received a W-2 form for 2015 to let them know about the attack.

Attribution 1 Publication: patch.com Author: Tony Schinella
Article Title: Concord School District Reports 'Data Security Breach'
Article URL: <http://patch.com/new-hampshire/concord-nh/concord-school-district-reports-data-security-breach-0>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-13	Single Digits	NH	5/19/2016	Electronic	Business	Yes - Unknown #	Unknown

On May 17, 2016, Single Digits fell victim to a phishing email purportedly coming from its chief executive officer. As a result, an unauthorized third party was emailed an electronic file containing certain information on individuals that were employed by Single Digits during 2015.

Attribution 1 Publication: NH AG's office Author:
Article Title: Single Digits
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/single-digits-20160519.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-12	Match-Up Solutions, LLC	FL	5/31/2016	Electronic	Business	Yes - Published #	3,078

On May 3, 2016, Match-Up teamed that online stores it maintained for one of its clients may have been compromised. Match-Up immediately took the sites offline and hired independent computer forensic experts to assist with its investigation. While the investigation is still ongoing, it appears that one or more unauthorized individuals may have gained access to the e-commerce platform and inserted malware that captured customers' names, addresses, credit and debit card numbers, security codes, and expiration dates at the point of check-out. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / IN AG' Author:
Article Title: Match-Up Solutions, LLC
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/match-up-solutions-20160526.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-11	Northwest Oncology & Hematology, S.C.	IL	5/11/2016	Electronic	Medical/Healthcare	Yes - Published #	1,625

Northwest Oncology & Hematology, S.C IL Healthcare Provider 1625 05/11/2016 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Northwest Oncology & Hematology, S.C.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-10	Edwin Shaw Rehabilitation	OH	4/22/2016	Electronic	Medical/Healthcare	Yes - Published #	975

Edwin Shaw Rehabilitation OH Healthcare Provider 975 04/22/2016 Loss Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Edwin Shaw Rehabilitation
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-09	AFLAC	GA	5/20/2016	Paper Data	Medical/Healthcare	Yes - Published #	930

Aflac GA Health Plan 930 05/20/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: AFLAC
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 133 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-08	Orchid MPS Holdings, LLC / Welfare Benefit Plan	MI	5/26/2016	Paper Data	Medical/Healthcare	Yes - Published #	771

Orchid MPS Holdings, LLC Welfare Benefit Plan MI Health Plan 771 05/26/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Orchid MPS Holdings, LLC / Welfare Benefit Plan
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-07	Sun Road	FL	6/1/2016	Paper Data	Business	Yes - Unknown #	Unknown

Owner Alfredo Bacci is accused of carelessly tossing his former employee's personal information into the trash while clearing out his business. Bacci said he did not toss the documents in the trash.

Attribution 1 Publication: WFTV.com Author:
Article Title: Oviedo business accused of placing former employees at risk of identity theft
Article URL: <http://www.wftv.com/news/local/oviedo-business-accused-of-placing-former-employees-at-risk-of-identity-theft/316309>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-06	CiCi's Pizza	TX	6/4/2016	Electronic	Business	Yes - Unknown #	Unknown

CiCi's Pizza, an American fast food business based in Coppell, Texas with more than 500 stores in 35 states, appears to be the latest restaurant chain to struggle with a credit card breach. The data available so far suggests that hackers obtained access to card data at affected restaurants by posing as technical support specialists for the company's point-of-sale provider, and that multiple other retailers have been targeted by this same cybercrime gang.

Attribution 1 Publication: krebsonsecurity.com / CA AG's office / S Author:
Article Title: Banks: Credit Card Breach at CiCi's Pizza
Article URL: <http://krebsonsecurity.com/2016/06/banks-credit-card-breach-at-cicis-pizza/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-05	Pennsylvania State University	PA	6/4/2016	Electronic	Educational	Yes - Published #	379

According to their report, the university was notified on April 13 that a historical document uploaded to the Undergraduate Law Society's web site was a spreadsheet that contained two fields – SSN and DOB – that were not visible on casual inspection, but could be “unhidden” in Excel. The records therefore exposed the SSN and DOB of 379 individuals. Upon notification, the university immediately took the site offline while they investigated.

Attribution 1 Publication: databreaches.net Author:
Article Title: Defunct undergrad law society site exposed hundreds of SSNs
Article URL: <http://www.databreaches.net/defunct-undergrad-law-society-site-exposed-hundreds-of-ssns/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-04	Cambridge Institute of International Education (CIIE)	MA	6/7/2016	Electronic	Educational	Yes - Unknown #	Unknown

The MacKeeper Security Research center experts have discovered and helped to secure a publicly available, non-password protected database containing more than a half of a million records on international students and info on 12 thousand host families and housing information.

Attribution 1 Publication: databreaches.net / mackeeper.com Author:
Article Title: Boston-based educational consulting firm exposed personal information of thousands of international students and hosting ho
Article URL: <https://mackeeper.com/blog/post/234-cambridge-institute-leaks-records-of-600-000-international-students>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-03	University of New Mexico Hospital	NM	6/7/2016	Paper Data	Medical/Healthcare	Yes - Published #	2,827

University of New Mexico Hospital has started notifying 2,827 patients of a breach of personal and medical information that first occurred in late December, 2015. Patients' names, service dates, providers' names, and brief descriptions of the medical services provided were detailed on invoice documents which were mailed out to 18 different addresses over a period of 15 weeks.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: University of New Mexico Hospital Privacy Breach
Article URL: <http://www.hipaajournal.com/two-healthcare-providers-announce-billing-related-phi-breaches-3462/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-02	Loyola University Medical Center	IL	6/7/2016	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

On April 5, 2016., Loyola University Medical Center discovered billing statements had been sent to incorrect addresses in February 2016. The University had undertaken a project to acquire accurate addresses; however, some billing statements ended up being released to addresses that had not been verified.

Attribution 1 Publication: hipaajournal.com / databreaches.net Author:
Article Title: Loyola University Medical Center Privacy Breach
Article URL: <http://www.hipaajournal.com/two-healthcare-providers-announce-billing-related-phi-breaches-3462/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160607-01	Empathia, Inc.	CA	6/3/2016	Electronic	Business	Yes - Published #	26,446

On January 30, 2016, we discovered spam files on one of our data servers. We removed the spam and immediately launched an investigation to determine the nature of the access and what data may have been stored on that server. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / IN AG' Author:
Article Title: Empathia, Inc.
Article URL: https://oag.ca.gov/system/files/Empathia%20-%20Notice%20of%20Data%20Event%20Notice%20Only-%20CA_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160606-01	ProMedica / Herrick Hospital	MI	6/3/2016	Electronic	Medical/Healthcare	Yes - Published #	3,472

ProMedica has recently discovered that seven of its employees had been improperly accessing the protected health information of patients for almost two years. That investigation revealed that the records of 3,500 patients had been improperly accessed over a period of two years, from May 1, 2014., to April 26, 2016. The type of data viewed by the employees include patients' names, addresses, dates of birth, contact telephone numbers, insurance information, medical diagnoses, details of medications that had been prescribed, and other clinical data.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: PROMEDICA UNCOVERS UNAUTHORIZED ACCESSING OF PHI BY 7 EMPLOYEES
Article URL: <http://www.hipaajournal.com/promedica-unauthorized-accessing-phi-7-employees-3457/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-10	Keystone Rural Health Consortia	PA	5/24/2016	Paper Data	Medical/Healthcare	Yes - Published #	800

A former employee stole a printout of a patient listing created in January 2015 that was hanging in the locked medical records room and used the information to send letters to several patients. The breach included the protected health information (PHI) of approximately 800 individuals and included demographic information, dates of birth, insurance information, and providers' names. The covered entity (CE), Keystone Rural Health Consortia, Inc., provided breach notification to HHS, affected individuals, and the media. OCR reviewed the CE's most recent risk analysis to ensure compliance with the Privacy and Security Rules and obtained assurances that the CE strengthened physical safeguards to prevent similar occurrences in the future.

Attribution 1 Publication: hhs.gov Author:
Article Title: Keystone Rural Health Consortia
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-09	Washington DC VA Medical Center	DC	5/31/2016	Paper Data	Government/Military	Yes - Published #	1,062

The Veterans Affairs Medical Center in Washington DC has notified 1,062 individuals of a possible data breach after an alleged theft, according to the OCR's website. In a statement, the Department of Veterans Affairs reported that it's privacy office was contacted on March 31 regarding a missing controlled substance monthly report. The document contained personal information on veterans, including first and last names as well as full and partial Social Security numbers.

Attribution 1 Publication: hhs.gov / healthitsecurity.com Author:
Article Title: Missing report leads to patient privacy violation at VA medical center
Article URL: <http://healthitsecurity.com/news/healthcare-system-break-ins-result-in-potential-phi-breaches>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-08	California Health & Longevity Institute / Bizmatics	CA	5/26/2016	Electronic	Medical/Healthcare	Yes - Published #	4,386

The clinic was notified on March 30, 2016, that cyber intruders may have installed malware into PrognoCIS that was not discovered by Bizmatics until the end of 2015. Bizmatics is working with law enforcement and a cyber-security firm on the matter but have been unable to conclude whether or not the clinic's patients' information was actually viewed or acquired.

Attribution 1 Publication: CHLI website / hipaaajournal.com Author:
Article Title: California Health & Longevity Institute
Article URL: http://www.chli.com/public_notice/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-07	Integrated Health Solutions / Bizmatics	PA	5/25/2016	Electronic	Medical/Healthcare	Yes - Published #	19,776

On March 30, 2016, Integrated Health Solutions, P.C. was informed by Bizmatics, Inc. ("Bizmatics"), our electronic medical records service provider, that it experienced unauthorized access to its records which may have included our patient records. This information may include name, address, social security number and health visit information.

Attribution 1 Publication: hhs.gov / the morning call Author:
Article Title: Integrated Health Solutions
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-06	Tumblr	NY	5/31/2016	Electronic	Business	Yes - Unknown #	Unknown

More than 65 million Tumblr accounts from a 2013 breach were spotted for sale on the dark web. Security researcher and Haveibeenpwned owner Troy Hunt recently found a database containing the stolen account information for sale on a dark web market site and listed the breach on his own site as the third largest ever.

Attribution 1 Publication: scmagazine.com Author:
Article Title: 65M Tumblr accounts for sale after 2013 breach
Article URL: <http://www.scmagazine.com/tumblr-accounts-from-2013-breach-for-sale-on-dark-web/article/499562/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-05	Myspace	CA	5/31/2016	Electronic	Business	Yes - Unknown #	Unknown

Usernames, passwords and email addresses registered before June 11, 2013 were compromised and were spotted on an online hacking forum, according to a May 31 Myspace blog post. Officials believe Russian cyberhacker 'Peace', who is allegedly responsible for the LinkedIn and Tumblr breaches, is also responsible for this event.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Time confirms Myspace breach, 360M accounts potentially affected
Article URL: <http://www.scmagazine.com/myspace-accounts-breach-confirmed-millions-of-accounts-potentially-compromised/artic>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-04	National Network of Abortion Funds	MA	5/27/2016	Electronic	Business	Yes - Unknown #	Unknown

On or about April 7, 2016, the National Network of Abortion Funds (NNAF) Bowl-a-Thon website (<http://bowlathon.nnaf.org/>) was attacked. Out of an abundance of caution, on April 14, 2016, we shut down the Bowl-a-Thon website in order to investigate the breadth and depth of this attack, working with law enforcement, forensic experts, legal counsel, and our website hosting vendor. As a result of this investigation, we learned on May 24, 2016 that certain donors' payment card information was compromised by a specific part of this broader attack. Specifically, the attacker injected malicious code that allowed the attacker to observe the information entered when the donations were made. We regret that your personal information and payment card information may be among those affected.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: National Network of Abortion Funds
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/National%20Network%20Of%20Abortion%20Funds%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-03	Stamford Podiatry Group / Bizmatics	CT	5/25/2016	Electronic	Medical/Healthcare	Yes - Published #	40,491

ased on our investigation to date, it appears that tmauthorized persons with unknown and potentially malicious intent gained covert access to our systems between February 22 and April 14, 2016, including the ability to access our electronic health records database. Although we have not been able to confirm that your personal information was accessed and copied, we have not been able to rule out that possibility and encourage you to take the protective measures described below. (Bizmatics)

Attribution 1 Publication: VT AG's office / Scmagazine.com / MD Author:
Article Title: Data of 40,000 Stamford Podiatry Group patients compromised
Article URL: <http://www.scmagazine.com/data-of-40000-stamford-podiatry-group-patients-compromised/article/500698/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-02	Shoes West Distribution Inc.	CA	5/31/2016	Electronic	Business	Yes - Unknown #	Unknown

On April25, 2016, we learned that our website may have been compromised. Taos Footwear immediately began an investigation and discovered that malicious code was installed on our website on April .14, 2016. We also found evidence that an unauthorized person may have gained access to some of your information.

Attribution 1 Publication: VT AG's office Author:
Article Title: Shoes West Distribution Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Shoes%20West%20Distribution%20%20Inc%20SBN%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160601-01	Verity Health System	OR	4/27/2016	Electronic	Medical/Healthcare	Yes - Published #	7,604

On May 22, 2016, we learned that a Verity employee was targeted on April 27, 2016, by an isolated email phishing scam in which an individual outside of Verity impersonated a Verity executive requesting certain information for Verity employees. The result of this scam was that certain information related to current and former employees who would have received a W-2 for 2015 was disclosed. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / hipaajournal.com / IN A Author:
Article Title: Verity Health System
Article URL: https://oag.ca.gov/system/files/Verity%20Health%20System%20-%20Sample%20Notice_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 137 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160531-09	AIM Inc.	IL	4/26/2016	Electronic	Business	Yes - Unknown #	Unknown

The investigation determined that the unauthorized person identified an issue in the document upload feature of the website server that customers used to upload license and age verification documents. For most individuals the information that was accessed included the customer's name and driver's license. For a small percentage of individuals the information that was accessed may have included their name and driver's license and/or state identification number, Social Security number, passport or military identification.

Attribution 1 Publication: NH AG's office / SC AG's office / MD AG Author:
Article Title: AIM Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/aim-20160426.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160531-08	Kline Galland / Caroline Kline Galland Home / Galland	WA	5/2/2016	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Paper records were stolen from a home care worker's vehicle, where the rear driver's side window was broken and items were removed from the vehicle, including the home care worker's work bag, which was located in the trunk. Also taken was a laptop computer containing PHI, but which we have determined was fully encrypted and did NOT contain the encryption key.

Attribution 1 Publication: WA AG's office Author:
Article Title: Kline Galland / Caroline Kline Galland Home / Galland Home Care Services
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/KlineGallandHome

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160531-07	Ameris Bank	FL	5/6/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On Thursday March 10, 2016, Ameris Bank discovered suspicious activity relating to one of their loan officer's email accounts. Ameris Bank immediately began an investigation into the nature and scope of this incident. Through the ongoing investigation, Ameris Bank determined that an unauthorized individual had gained access to the loan officer's email account from February 2, 2016 to March 10, 2016, and that information contained in the email account was accessible to the unauthorized individual for this period of time.

Attribution 1 Publication: WA AG's office Author:
Article Title: Ameris Bank
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/AmerisBank2016-05

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160531-06	Macfadden	MD	5/26/2016	Electronic	Business	Yes - Unknown #	Unknown

I regret to inform you that an internal investigation has confirmed that Macfadden has suffered a data breach of employee information. Based on our investigation, we have learned that sometime in April of this year, some employees' personally identifiable information has been compromised when it was improperly downloaded from an online offsite backup storage system used by a former employee who had access to this data. While this matter is subject to an ongoing investigation, we have determined that it is best to inform all affected parties of the potential exposure of your respective personal information and to take steps to mitigate this risk.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: Macfadden
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Macfadden%20Inc%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160531-05	Department of Agriculture	OH	5/29/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

The 13abc I-Team has uncovered a major personal information release by the State of Ohio. Drivers' licenses, social security numbers, even birth certificates without personal information blocked out was all released by the Department of Agriculture.

Attribution 1 Publication: databreaches.net / 13abc.com Author:
Article Title: Major personal information release by state of Ohio
Article URL: <http://www.13abc.com/home/headlines/Major-personal-information-release-by-state-of-Ohio-322449662.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160531-04	Emergency Medicine Associates (Carondelet)	AZ	5/30/2016	Electronic	Medical/Healthcare	Yes - Published #	1,067

Approximately 1,000 patients in Southern Arizona have been notified of a breach of protected health information following the theft of a physician's logbook. The logbook had been left in the vehicle of a physician who worked for Emergency Medicine Associates, which provided ER staff for Carondelet Health Network hospitals in Tucson, Arizona. A thief broke into the physician's vehicle on or around March 25, 2016 and took the logbook. (Carondelet)

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Tucson Emergency Room Patients' PHI Stolen from Physician's Vehicle
Article URL: <http://www.hipaajournal.com/tucson-emergency-room-patients-phi-stolen-from-physicians-vehicle-3449/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160531-03	Tallahassee Memorial Healthcare, Inc.	FL	5/20/2016	Electronic	Medical/Healthcare	Yes - Published #	505

Tallahassee Memorial HealthCare, Inc., the covered entity (CE), discovered that an employee attempted to upload protected health information (PHI) containing patients' names, insurance numbers, payor financial information numbers, and account numbers to an unauthorized website. The breach affected 505 individuals. The CE sent timely breach notification to HHS and to affected individuals and provided free credit monitoring to affected individuals. In response to the breach, the CE sanctioned the responsible employee, flagged patient accounts in its internal billing system, revised its website filter to block additional web sites, and updated its employee training. OCR obtained assurances from the CE that it implemented the corrective actions listed above.

Attribution 1 Publication: hhs.gov Author:
Article Title: Tallahassee Memorial Healthcare, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160531-02	Surgical Care Affiliates	AL	5/16/2016	Electronic	Medical/Healthcare	Yes - Published #	9,009

Surgical Care Affiliates AL Business Associate 9009 05/16/2016 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Surgical Care Affiliates
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160531-01	Associates in EyeCare, PSC	KY	5/16/2016	Electronic	Medical/Healthcare	Yes - Published #	971

An office of the covered entity (CE), Associates in EyeCare, P.S.C., was broken into and two laptop computers and an external hard drive were stolen. The breach affected 971 individuals and the types of protected health information (PHI) involved in the breach included patients' names, internal account numbers, optical images, technical information about the images, and dates of birth. The CE provided timely breach notification to HHS, affected individuals, and the media. The CE also posted notification about the breach to its website.

Attribution 1 Publication: hhs.gov Author:
Article Title: Associates in EyeCare, PSC
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160525-01	Lewis-Palmer School District 38	CO	5/24/2016	Electronic	Educational	Yes - Published #	2,000

Lewis-Palmer School District 38 officials are mum about the probability that a security breach related to its Infinite Campus platform may have compromised more than 2,000 students' personal information. Infinite Campus is a software program that stores personal and academic information about students in the district. Many districts use the system, but those districts are free to decide how much information is accessible to parents and students online. Many districts only allow access to grades, attendance, and schedules. Lewis-Palmer extends the information to highly confidential personal information.

Attribution 1 Publication: completecolorado.com Author: Sherrie Peif
 Article Title: Probable security breach may have compromised thousands of Lewis Palmer students' data
 Article URL: <http://completecolorado.com/pagetwo/2016/05/24/probable-security-breach-may-have-compromised-thousands-of-lew>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-18	UnitedHealth Group Single Affiliated Covered Entity	MN	5/4/2016	Paper Data	Medical/Healthcare	Yes - Published #	5,330
UnitedHealth Group Single Affiliated Covered Entity (SACE) MN Health Plan 5330 05/04/2016 Unauthorized Access/Disclosure Paper/Films							

Attribution 1 Publication: hhs.gov Author:
 Article Title: UnitedHealth Group Single Affiliated Covered Entity (SACE)
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-17	Southeast Eye Institute, PA dba Associates of Pinellas /	FL	5/5/2016	Electronic	Medical/Healthcare	Yes - Published #	87,314
Southeast Eye Institute, P.A. dba eye Associates of Pinellas FL Healthcare Provider 87314 05/05/2016 Hacking/IT Incident Network Server (Bizmatics)							

Attribution 1 Publication: hhs.gov Author:
 Article Title: Southeast Eye Institute, PA dba Associates of Pinellas / Bizmatics
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-16	Lafayette Pain Care PC / Bizmatics	IN	5/9/2016	Electronic	Medical/Healthcare	Yes - Published #	7,500
Lafayette Pain Care was informed by Bizmatics that it had been affected by the security breach and hackers had probed the server on which the patients' data were stored. Lafayette Pain Care had issued a statement saying the investigation into the breach suggests that Lafayette's data were not in fact compromised or obtained by hackers.							

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
 Article Title: Lafayette Pain Care PC
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-15	Family Medicine of Weston / Bizmatics	FL	5/11/2016	Electronic	Medical/Healthcare	Yes - Published #	500
Family Medicine of Weston FL Healthcare Provider 500 05/11/2016 Hacking/IT Incident Electronic Medical Record							

Attribution 1 Publication: hhs.gov Author:
 Article Title: Family Medicine of Weston / Bizmatics
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-14	Employee Benefits Division	AR	5/12/2016	Electronic	Medical/Healthcare	Yes - Published #	2,602
Employee Benefits Division AR Health Plan 2602 05/12/2016 Unauthorized Access/Disclosure Email							

Attribution 1 Publication: hhs.gov Author:
 Article Title: Employee Benefits Division
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 140 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-13	Coordinated Health Mutual, Inc.	OH	5/20/2016	Paper Data	Medical/Healthcare	Yes - Published #	591

Coordinated Health Mutual, Inc. OH Health Plan 591 05/20/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Coordinated Health Mutual, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-12	ABCya.com	RI	5/20/2016	Electronic	Business	Yes - Unknown #	Unknown

ABCya had the credit card data stored on a misconfigured database that was publically available: credentials and info of 11k+ archived customers (incl. IPs, emails, names, temporary access code, hashed and salted passwords); credentials and info on 21k+ active customers (incl. credit cards details such as hashed ID, fingerprints, expiration year and month, last 4 digits and card name in plain text); more than 3k+ Stripe tokens and info; and credentials of 4 "super admin" users for ABCya with encrypted/salted passwords and details.

Attribution 1 Publication: databreaches.net / MackKeeper Security Author:
Article Title: Children's Educational Site Exposes Thousands of User Accounts and Payment Data
Article URL: <https://mackeeper.com/blog/post/224-childrens-educational-site-exposes-thousands-of-user-accounts-and-payment-d>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-11	Comanche County Memorial Hospital / Memorial Medical	OK	5/19/2016	Electronic	Medical/Healthcare	Yes - Published #	2,199

On February 26, 2016, the company contracted to provide patient satisfaction surveys for the MMG determined that an e-mail survey sent to numerous patients included incorrect information. The surveys did not include any diagnoses or dates the physician was seen. They also did not contain any insurance or financial information of either the individual to whom the survey was sent or the individual whose name was in the subject line of the e-mail. They also did not include any identifying information about the individual other than the individual's name. No social security numbers, addresses or phone numbers were disclosed.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Comanche County Memorial Hospital notifies 2,199 patients after contractor's email gaffe
Article URL: <http://www.databreaches.net/comanche-county-memorial-hospital-notifies-2199-patients-after-contractors-email-gaffe/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-10	El Paso Independent School District	TX	5/23/2016	Electronic	Educational	Yes - Unknown #	Unknown

In mid-April, computer hackers had five days' access to the personal data of a reported 51 El Paso Independent School District employees and were able to redirect their April 15 paychecks.

Attribution 1 Publication: databreaches.net / elpasoinc.com Author:
Article Title: EPISD employee accounts hacked, money stolen
Article URL: http://www.elpasoinc.com/news/local_news/article_9c0a4f3a-20fe-11e6-b531-d7817e7eb054.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-09	Puppet, Inc.	TX	5/9/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 13, 2016, we learned that an employee had responded to a "phishing" email on March 1, 2016, thinking that it was a legitimate request. When we learned of this, we immediately secured the email account, reset passwords and began an investigation of the incident. Our investigation revealed that the employee inadvertently disclosed a copy of information included on your 2015 W-2 form, which includes your name, Social Security number, and salary information.

Attribution 1 Publication: OR AG's office / MD AG's office Author:
Article Title: Puppet, Inc.
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1046511380>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-08	Milwaukee Bucks	WI	5/19/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 26 an unknown party requested the documents from the Bucks via email, using a spoof email address to impersonate Peter Feigin, the team's president. An employee responded to that email request, not knowing that it was from a fraudulent source, and provided the documents, according to the team statement.

Attribution 1 Publication: USA Today.com Author: Charles Gardner
 Article Title: Milwaukee Bucks the victims of serious financial security breach
 Article URL: <http://www.usatoday.com/story/sports/nba/bucks/2016/05/19/milwaukee-bucks-victims-serious-financial-security-brea>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-07	Maritz Holdings, Inc.	MO	5/23/2016	Electronic	Business	Yes - Published #	1,871

On April 7, 2016, we learned that a possible data security incident which occurred between March 1 and March 17, 2016 may have impacted documents that were stored in our system. With the help of outside forensic computer experts, we conducted an investigation to determine what information, specifically, may have been affected. Unfortunately, it appears these documents may have contained a limited amount of your personal information. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / MD AG's office / IN AG' Author:
 Article Title: Maritz Holdings, Inc.
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Maritz%20Holdings%20Inc%20SBN%20to%20Consume

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-06	A&A Ready Mixed Concrete, Inc.	CA	5/16/2016	Electronic	Business	Yes - Unknown #	Unknown

We are contacting you regarding a data security incident that occurred on Monday, May 16th, 2016, at the Company. It appears the targeted data involved 2015 W2 information of employees which could potentially become available to unknown individuals. As a result, your personal information may have been exposed to others. Please be assured we have taken every step necessary to address the incident, and are fully committed to protecting your information.

Attribution 1 Publication: CA AG's office Author:
 Article Title: A&A Ready Mixed Concrete, Inc.
 Article URL: https://oag.ca.gov/system/files/DATABREACH_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-05	Berkeley Endocrine Clinic	CA	4/22/2016	Electronic	Medical/Healthcare	Yes - Published #	1,370

On April 22, 2016, my office was subject to a spam email which we believe went to many patients. Though no patient information was affected by that correspondence, we sent a notification email to all individuals on our email list, informing them of the spam. Inadvertently, the recipient list for the notification email on April 22, 2016 was not hidden.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Berkeley Endocrine Clinic
 Article URL: https://oag.ca.gov/system/files/Berkeley%20Endocrine%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-04	San Juan County	NM	5/23/2016	Electronic	Government/Military	Yes - Published #	12,500

A hacking incident has resulted in a potential healthcare data breach for alcohol and substance abuse patients in San Juan County, New Mexico. In an official statement on its website, San Juan County announced that an outside entity had gained access to a county-owned computer, which contained PHI. The hacker was able to access the computer for approximately half an hour.

Attribution 1 Publication: modernhealthcare.com Author: Joseph Conn
 Article Title: Data breach affects 12,000 patients in New Mexico substance-abuse program
 Article URL: <http://www.modernhealthcare.com/article/20160523/NEWS/160529984/data-breach-affects-12000-patients-in-new-mexi>

Attribution 2 Publication: HealthITSecurity.com Author: Jacqueline Belliveau
 Article Title: NM county reports healthcare data breach after hacking incident
 Article URL: <http://healthitsecurity.com/news/malware-incident-in-mi-creates-potential-phi-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-03	Complete Chiropractic and Bodywork Therapies	MI	5/23/2016	Electronic	Medical/Healthcare	Yes - Published #	4,082

According to the OCR's data breach portal, approximately 4,082 individuals were affected by the healthcare data security event. Complete Chiropractic and Bodywork Therapies reported that an outside party had gained access to a server containing PHI starting on November 19, 2015. The practice did not discover the intrusion until after the server malfunctioned on March 19, 2016.

Attribution 1 Publication: healthitsecurity.com Author: Jacqueline Belliveau
 Article Title: Malware Incident in MI Creates Potential PHI Data Breach
 Article URL: <http://healthitsecurity.com/news/malware-incident-in-mi-creates-potential-phi-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-02	Noodles & Company	CO	5/23/2016	Electronic	Business	Yes - Unknown #	Unknown

"We have received information from Visa that during a recent security review, your Visa card number was identified as possibly being compromised at Noodles & Company locations and is at risk for unauthorized charges. Don't worry — you won't have to worry about paying for unauthorized charges because your card is backed by Visa's Zero Liability protection (some limitations apply)," reads an e-mail sent to a customer Monday by Denver Community Credit Union. The bank is sending a new credit card.

Attribution 1 Publication: denverpost.com / OR AG's office / NH A Author:
 Article Title: Noodles & Company indirectly warns customers of credit card breach
 Article URL: <http://www.denverpost.com/2016/05/23/noodles-company-indirectly-warns-customers-of-credit-card-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160524-01	O'Charley's Restaurants	GA	5/20/2016	Electronic	Business	Yes - Unknown #	Unknown

When one of our network security tools identified suspicious network traffic, we immediately began an investigation and engaged a leading third party cyber-security firm to assist. On April 8, 2016, the cyber-security investigation identified signs of unauthorized access to the payment card network of our restaurants. Findings show that an unauthorized program was installed on point-of-sale devices that looked for data from payment cards swiped in the restaurants when the data was being routed to obtain authorization for the transaction. In some instances the program identified data from the card's magnetic stripe that included the cardholder name and card number. In other instances the program only found data from the magnetic stripe that did not include the cardholder name.

Attribution 1 Publication: GA AG's office / O'Charley's website Author:
 Article Title: O'Charley's Restaurants
 Article URL: <http://www.ocharleys.com/protectingourguests>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160523-04	Conway Group, Inc.	MD	5/16/2016	Electronic	Business	Yes - Unknown #	Unknown

On May 11, 2016, Conway learned that a Conway employee was the target of a "phishing" attack on April 29, 2016. The employee received an e-mail from a "spoofed" e-mail address, which asked for employees' W-2 information. The employee, believing the e-mail to be a legitimate request from a Conway executive, responded to the e-mail. As a result of this "phishing" incident, Conway employees' federal form W-2s, which include name, address, and social security number, may have been exposed to an unknown and unauthorized party.

Attribution 1 Publication: NH AG's office Author:
 Article Title: Conway Group
 Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/conway-group-20160516.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 143 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160523-03	Paper Works	CA	5/6/2016	Electronic	Business	Yes - Unknown #	Unknown

We were the victim of an office break in on March 30, 2016. Among the items stolen were a laptop and a computer tower containing sensitive customer information. This information includes name, address and social security number information for you, as well as any spouse and dependents that may be listed on your tax filing.

Attribution 1 Publication: CA AG's office Author:
Article Title: Paper Works
Article URL: https://oag.ca.gov/system/files/Paper%20Tree%20resubmit-%20adults%20only_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160523-02	Flurish, Inc. dba LendUp	CA	5/11/2016	Electronic	Business	Yes - Unknown #	Unknown

Earlier this year during a routine examination, we discovered that personal information for a small subset of visitors to our website had been made available to third-party companies. We place on our website widgets, beacons, and analytics trackers from third-party companies to provide services to us and our customers related to device authentication, site functionality, advertising, and marketing. Our examination showed that personal information could have been made available to these third-party companies, for a small number of customers, as early as 2012.

Attribution 1 Publication: CA AG's office Author:
Article Title: Flurish, Inc. dba LendUp
Article URL: https://oag.ca.gov/system/files/CA%20Consumer%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160523-01	H&R Block	MO	5/16/2016	Electronic	Business	Yes - Unknown #	Unknown

At H&R Block, we value your business and are writing to inform you of a recent issue potentially involving your personal information. Protecting your privacy is very important to us, please review the included notice regarding a former H&R Block Expat Tax Services employee who took various files and information for the purpose of starting a competing tax preparation company. This information may have included personal information about you, including information typically used to file U.S. tax returns.

Attribution 1 Publication: VT AG's office Author:
Article Title: H&R Block
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/H&R%20Block%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160517-04	Digilant	MA	5/6/2016	Electronic	Business	Yes - Unknown #	Unknown

On May 3, 2016, we discovered that our company was the targeted victim of an email spoofing attack that compromised the security of your 2015 W-2 record, which contains your name, address, Social Security number, and 2015 compensation information. This attack occurred on March 30, 2016. We are working diligently to mitigate the impact of this event and we are notifying you so that you can take action, along with our efforts, to minimize any potential for personal financial harm.

Attribution 1 Publication: NH AG's office Author:
Article Title: Digilant
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/digilant-20160606.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160517-03	Bingham Junior High	MO	5/16/2016	Electronic	Educational	Yes - Unknown #	Unknown

Former students and parents want to know why student records with personal information are sitting inside an abandoned school at 77th and Wyandotte in Kansas City, Mo. The former Bingham Junior High School building closed in 2001, but an anonymous source gave FOX 4 a box of files containing student names, social security numbers, birth certificates and medical records. Some of the files are for students that attended the school, but other files are contain information on students who were in a program operated by the Kansas City, Mo. School District.

Attribution 1 Publication: fox4kc.com / databreaches.net Author: Monica Evans
Article Title: After school closes its doors, personal student records remain inside, unprotected
Article URL: <http://fox4kc.com/2016/05/16/trashed-13/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160517-02	Poway Unified School District	CA	5/16/2016	Electronic	Educational	Yes - Published #	36,000

The Poway Unified School District released to one parent in the district sensitive personal information about more than 36,000 children, in response to a public-records request. The release was a mistake, as the parent asked for information about records containing her own name, and the district gave her much broader data sets containing the information about herself and others. The data included children's names, nicknames, addresses, phone numbers, hearing and vision exam results, dates of birth, language fluency, academic test results and occupation of parents, according to the woman who received the data, Gabriela Dow.

Attribution 1 Publication: San Diego Union-Tribune Author: Daniel Wheaton
Article Title: Poway data breach affects 30,000-plus students
Article URL: <http://www.sandiegouniontribune.com/news/2016/may/16/poway-data-breach/?Watchdog-article-copy>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160517-01	Zocdoc, Inc.	NY	5/16/2016	Electronic	Medical/Healthcare	Yes - Published #	17,000

In June 2015, we learned of programming errors in the processes responsible for managing username access to the Provider Dashboard. This allowed some past or current practice staff members to access the Provider Dashboard, and therefore potentially view your personal information, after their usernames were removed, deleted or otherwise limited. Access may have occurred between [first access date] to [last access date]. These practices and their staff members had obligations regarding the secure and confidential handling of personal information. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: Zocdoc, Inc.
Article URL: https://oag.ca.gov/system/files/CA%20Consumer%20Notification%20Zocdoc_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160516-06	Southern Michigan Bank & Trust	MI	5/13/2016	Electronic	Banking/Credit/Financial	Yes - Published #	38,601

A Southern Michigan Bank & Trust employee's vehicle was burglarized and a laptop stolen on April 10. The bank says there is no indication of a data breach, but staff are doing what they can to protect customers. The laptop's contents included names, checking account numbers and social security numbers, but no personal identification numbers (PINs) or passcodes. (Consumers affected per IN AG's office)

Attribution 1 Publication: databreaches.net / threeriversnews.com Author:
Article Title: Southern Michigan Bank & Trust notifies customers of stolen laptop
Article URL: http://www.threeriversnews.com/articles/2016/05/13/news/local_news/doc5735dec470ced539112232.txt

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160516-05	Imperial Valley Family Care Medical Group	CA	5/14/2016	Electronic	Medical/Healthcare	Yes - Published #	649

On March 21, 2016 there was a burglary at the office of Dr. Sampat and a single laptop computer was taken from the premises. A police report of the incident was filed with the El Centro Police Department. We have discovered during our investigation of the incident that the laptop may have contained patient's personal information, including name, address, date of birth, and personal health information. However, we have not received any indication that the information has been accessed or used by an unauthorized individual.

Attribution 1 Publication: Company website / databreaches.net / h Author:
Article Title: Imperial Valley Family Care Medical Group notifies patients after office burglary
Article URL: http://www.ivfcmg.com/docs/breach_notification.pdf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 145 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160516-04	PruittHealth Home Health - Low Country	SC	5/13/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,500

On the night of March 2, 2016, the offices of PruittHealth Home Health – Low Country were broken into by thieves. The perpetrators broke the glass of the front door and entered the offices. Nothing was stolen but petty cash. The thieves had the opportunity to access all of the medical records kept in the office, although it does not appear that any medical records were taken or even disturbed. The types of personal information that could have been accessed include things like patient names, addresses, social security numbers, dates of birth, dates of service, location of service, and other clinical information. Again, there is no indication that any of this information was actually accessed by the perpetrators.

Attribution 1 Publication: [databreaches.net / hhs.gov](#) Author:
Article Title: [PruittHealth Home Health – Low County notifies patients after office burglary](#)
Article URL: <http://www.databreaches.net/pruithhealth-home-health-low-county-notifies-patients-after-office-burglary/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160516-03	NTT Data	TX	5/4/2016	Electronic	Business	Yes - Published #	1,493

This letter is being sent in accordance with state law to inform your office that our company recently suffered an email spoofing incident that resulted in an employee unwittingly sending an unknown outside third party W -2 information about one (1) state resident on about April 22, 2016 in response to an email request that appeared to be from a company executive. (Consumers affected per IN AG's office)

Attribution 1 Publication: [N AG's office / IN AG's office](#) Author:
Article Title: [NTT Data](#)
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/ntt-data-20160504.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160516-02	California Correctional Health Care Services	CA	2/25/2016	Electronic	Government/Military	Yes - Published #	400,000

On April 25, 2016 California Correctional Health Care Services (CCHCS) identified a potential breach of your Personally Identifiable Information and Protected Health Information that occurred on February 25, 2016. An unencrypted laptop was stolen from a CCHCS workforce member's personal vehicle. The laptop was password protected in accordance with state protocol.

Attribution 1 Publication: [CA AG's office / hipaajournal.com](#) Author:
Article Title: [California Correctional Health Care Services](#)
Article URL: https://oag.ca.gov/system/files/CCHCS%20Breach%20Notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160516-01	City College of San Francisco	CA	5/13/2016	Electronic	Educational	Yes - Unknown #	Unknown

On April 15, 2016, we learned that an employee had responded to a “phishing” email thinking that it was a legitimate request. When we learned of this, we immediately secured the email account, reset passwords and began an investigation of the incident. We conducted a thorough review of the employee's e-mail account and confirmed that the emails contained student information and may have included your name, address, Social Security number, and other information contained in your application for financial aid.

Attribution 1 Publication: [CA AG's office / MD AG's office](#) Author:
Article Title: [City College of San Francisco](#)
Article URL: https://oag.ca.gov/system/files/Adult%20CA%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160513-06	RugDoctor	TX	5/10/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 15, 2016, we learned that Rug Doctor's 2015 W-2 tax form information for current and former U.S.-based employees was sent to an unauthorized third party in response to a phishing email scam. The information was sent by an employee who believed the phishing email was a legitimate internal company request. The scam took place on March 8, 2016.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: RugDoctor
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/rugdoctor-20160510.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160513-05	Kern County Superintendent of Schools	CA	5/12/2016	Electronic	Educational	Yes - Published #	2,500

Employees of Kern Superintendent of Schools have been alerted to a data breach at the organization, 23ABC News has learned. In a note sent to staff members on Monday, Superintendent Christine Lizardi Frazier said the group's payroll department fell victim to a data phishing scam. A KCSOS spokesman told 23ABC the incident happened on Friday, May 6, and employees were also notified that day about the breach.

Attribution 1 Publication: databreaches.net / turnto23.com Author:
Article Title: KCSOS investigating employee data breach
Article URL: <http://www.turnto23.com/news/local-news/kcsos-investigating-employee-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160513-04	Avention (formerly OneSourceSolutions)	MA	5/13/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 28, 2016, Avention learned that it suffered a data security incident, which resulted in unauthorized access to employees' 1-9 Forms by an unknown source on or around March 31, 2016. Immediately upon learning this information, Avention launched an internal investigation, contacted federal law enforcement, and hired a leading cybersecurity firm to assist with our investigation. In conducting our investigation, Avention learned that, on April 5, 2016, an Avention employee fell victim to a phishing attack, which resulted in the unauthorized disclosure of 2015 W-2 Forms

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Avention (formerly OneSourceSolutions)
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/avention-20160509.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160513-03	Washington Elementary School District Breach	AZ	4/15/2016	Electronic	Educational	Yes - Unknown #	Unknown

"Washington Elementary School District (WESD) administration discovered Tuesday afternoon, April 12, that a report of 2015 W-2 information was sent earlier that day to a fraudulent email address set up to appear as the superintendent's email address. The district immediately began to take corrective steps and notified law enforcement and the IRS. Notification has gone out to current and former employees who worked for WESD at any time between January 1 and December 31, 2015.

Attribution 1 Publication: azfamily.com Author:
Article Title: WESD employees' W-2 information compromised in phishing scheme
Article URL: <http://www.azfamily.com/story/31738609/wesd-employees-w-2-information-compromised-in-phishing-scheme>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160513-02	Kalamazoo College	MI	5/11/2016	Electronic	Educational	Yes - Published #	1,634

On April 29, 2016, we learned that a targeted "spear phishing" email message had been sent to a Kalamazoo College employee on the afternoon of April 28, 2016. Spear phishing emails are an attempt by an individual or group to solicit personal information from unsuspecting users by posing as someone known to the recipient. The email our employee received was designed to appear as though it had been sent by a Kalamazoo College administrator and requested faculty, staff and student employees' 2015 IRS Form W-2 Wage and Tax Statements. Believing the email to be legitimate, the employee replied to the message and attached the 2015 IRS Forms W-2, which included your name, address, Social Security number, and earnings information. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / IN AG's office Author:
Article Title: Kalamazoo College
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Kalamazoo%20College%20SBN%20to%20Consumers.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160513-01	Office of Lynn N. Talbott, Jr. CPA	CA	5/16/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 19, 2016, I detected suspicious activity on a work computer. I immediately took the computer off-line and contacted our IT consultant. The consultant has confirmed unusual activity and changed potentially impacted passwords. Further, on April 21, 2016, after a thorough analysis of the computer, the consultant removed malware found on the impacted computer's hard drive, and confirmed all firewalls and security protections were properly functioning.

Attribution 1 Publication: CA AG's office / databreaches.net Author:
 Article Title: Office of Lynn N. Talbott, Jr. CPA
 Article URL: https://oag.ca.gov/system/files/Talbott%20Notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160512-07	ADP	NJ	5/5/2016	Electronic	Business	Yes - Unknown #	Unknown

Payroll processing provider ADP has confirmed fraudsters gained access to some clients' online portals and compromised the W-2 data of employees at more than a dozen customer firms. According to ADP, however, the theft occurred after the impacted companies mistakenly published unique access codes to employee accounts online. The New Jersey-based company provides payroll, tax and benefits administration services to more than 640,000 businesses and corporations – one of them being U.S. Bank, where an estimated 1,400 employees were affected. (US Bank)

Attribution 1 Publication: MD AG's office Author:
 Article Title: ADP
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-270422.pdf>

Attribution 2 Publication: tripwire.com Author:
 Article Title: Identity Thieves Breach Payroll Service Provider ADP, Steal W-2 Data
 Article URL: <http://www.tripwire.com/state-of-security/latest-security-news/identity-thieves-breach-payroll-service-provider-adp-ste>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160512-06	Medical Colleagues of Texas	TX	5/11/2016	Electronic	Medical/Healthcare	Yes - Published #	68,631

Computer forensics experts were called in after an office employee at the family practice and obstetrics group noticed unusual activity on March 8 and it was determined the system had been hacked, Medical Colleagues of Texas said. The breached information could include names, addresses, health insurance information and Social Security numbers.

Attribution 1 Publication: houstonchronicle.com / NH AG's office / Author:
 Article Title: Data breach reported at Katy physicians group
 Article URL: <http://www.houstonchronicle.com/business/medical/article/Data-breach-reported-at-Katy-physicians-group-7463224.p>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160512-05	Children's National Health System / Ascend Healthcare	DC	5/11/2016	Electronic	Medical/Healthcare	Yes - Published #	4,107

Washington D.C.-based Children's National Health System (CNHS) has alerted patients to a breach of their protected health information following an error by a transcription service provider which allowed patients' data to be indexed by the search engines. CNHS is one of a number of healthcare clients affected by the data breach.

Attribution 1 Publication: healthinfosecurity.com Author:
 Article Title: Transcribed Medical Records Exposed on the Web
 Article URL: http://www.healthcareinfosecurity.com/transcribed-medical-records-exposed-on-web-a-9096?rf=2016-05-12-eh&mkt_to

Attribution 2 Publication: hipaajournal.com Author:
 Article Title: Transcription Service Provider Exposes PHI of Children's National Health System Patients
 Article URL: <http://www.hipaajournal.com/transcription-service-provider-exposes-phi-of-childrens-national-health-system-patients->

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160512-04	UnityPoint Health / Allen Hospital	IA	5/12/2016	Electronic	Medical/Healthcare	Yes - Published #	1,620

An employee of UnityPoint Health's Allen Hospital in Waterloo, Iowa, was recently discovered to have abused her access rights to patient health information over a period of seven years. During that time, the employee is understood to have improperly accessed the protected health information of 1,620 patients.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: UnityPoint Health's Allen Hospital Discovers 7-Year Privacy Breach
Article URL: <http://www.hipaajournal.com/unitypoint-healths-allen-hospital-discovers-7-year-privacy-breach-3427/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160512-03	Office of Mark Anthony Quintero, MD, LLC / Bizmatics	FL	4/12/2016	Electronic	Medical/Healthcare	Yes - Published #	650

Mark Anthony Quintero, M.D., L.L.C. FL Healthcare Provider 650 04/12/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Mark Anthony Quintero, MD, LLC / Bizmatics
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160512-02	Florida Medical Clinic, PA / Greenway Health	FL	5/12/2016	Electronic	Medical/Healthcare	Yes - Published #	1,000

Please be advised from November 18th, 2015 to January 6th, 2016 your Florida Medical Clinic, PA patient due balance statement (sample statement attached) was accessible to industrial account patients who logged onto the Patient Portal. Upon investigation, Florida Medical Clinic, PA discovered a setting was turned on by our Patient Portal vendor Greenway Health. Florida Medical Clinic, PA immediately shut down the setting and the issue is now resolved. Please know Florida Medical Clinic, PA takes these matters very seriously and has implemented additional protocols with Greenway Health to prevent any further occurrences.

Attribution 1 Publication: databreaches.net / FMC website Author:
Article Title: Florida Medical Clinic, PA notifies 1,000 patients after Greenway Health error exposed PHI
Article URL: <http://www.databreaches.net/florida-medical-clinic-pa-notifies-1000-patients-after-greenway-health-error-exposed-phi/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160512-01	San Mateo Foster City School District	CA	5/12/2016	Electronic	Educational	Yes - Unknown #	Unknown

The San Mateo Foster City School District (SMFCSD) reported that personal information of active employees was compromised when a thumb drive containing the sensitive data was lost.

Attribution 1 Publication: scmagazine.com Author: Robert Abel
Article Title: San Mateo Foster City School District employee PII compromised in breach
Article URL: <http://www.scmagazine.com/san-mateo-foster-city-school-district-employee-pii-compromised-in-breach/article/496000/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160510-10	City of Houston	TX	5/10/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

The names, social security numbers and other financial information was stored in a locked filing cabinet sold by the city at auction in February.

Attribution 1 Publication: databreaches.net / 12newsnow.com Author:
Article Title: Personal information of hundreds of City of Houston employees exposed
Article URL: <http://www.12newsnow.com/story/31934362/personal-information-of-hundreds-of-city-of-houston-employees-exposed>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 149 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160510-09	National Counseling Group	VA	3/21/2016	Electronic	Medical/Healthcare	Yes - Published #	23,000

On or about January 21, 2016, NCG determined that an unknown actor accessed certain employee email accounts in order to send phishing emails from those accounts to certain individuals affiliated with NCG

Attribution 1 Publication: hhs.gov / MD AG's office Author:
Article Title: National Counseling Group
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2016/itu-266973.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160510-06	Family & Children's Services of Mid Michigan, Inc.	MI	4/27/2016	Electronic	Medical/Healthcare	Yes - Published #	981

Family & Children's Services of Mid Michigan, Inc. MI Healthcare Provider 981 04/27/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Family & Children's Services of Mid Michigan, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160510-05	Northstar Healthcare Acquisitions LLC / Equalize	TX	4/28/2016	Electronic	Medical/Healthcare	Yes - Published #	19,898

A laptop computer containing the electronic protected health information (ePHI) of 19,898 individuals was stolen from vehicle of an employee of Equalize Revenue Cycle Management (ERCM). ERCM is a business associate (BA) of Northstar Healthcare Acquisitions, LLC, the covered entity (CE). The ePHI included insurance and treatment information and other demographic information. Upon discovering the breach, the BA informed law enforcement. The BA notified the affected individuals, provided substitute notice via its website, and media notification. The BA offered one year of free credit monitoring services to affected individuals.

Attribution 1 Publication: hhs.gov Author:
Article Title: Northstar Healthcare Acquisitions LLC / Equalize Revenue Cycle Management
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160510-04	Managed Health Services	IN	5/1/2016	Paper Data	Medical/Healthcare	Yes - Published #	610

Managed Health Services IN Health Plan 610 05/01/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Managed Health Services
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160510-03	Mayfield Clinic of Cincinnati	OH	5/10/2016	Electronic	Medical/Healthcare	Yes - Published #	23,341

In February, patients of the Mayfield Clinic of Cincinnati, Ohio were sent an email containing a malicious attachment which downloaded ransomware onto their devices. The entry on the HHS' Office for Civil Rights breach portal indicates 23,341 patients were sent the email, although it is unclear how many email recipients opened the malicious attachment and infected their computers. The email was sent by an individual who gained access to a database held by one of Mayfield's vendors.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 23K Patients of Mayfield Clinic Sent Malware-Infected Email
Article URL: <http://www.hipaajournal.com/23k-patients-mayfield-clinic-sent-malware-infected-email-3422/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 150 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160510-02	Strafaci & Associates	FL	5/3/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 17, 2016, we learned that a "phishing" email was sent to an employee who responded to the email thinking it was a legitimate request. When we learned of this, we immediately secured the email account, reset passwords and began an investigation. We also engaged an outside forensic firm to assist in the investigation, help determine which email accounts may have been affected, and to identify individuals whose information may have been accessible.

Attribution 1 Publication: NH AG's office Author:
Article Title: Strafaci & Associates
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/strafaci-associates-20160503.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160510-01	New Hampshire Distributors	NH	4/26/2016	Electronic	Business	Yes - Unknown #	Unknown

On or about April 6, 2016, the vehicle of a Daystar employee, who was in charge of securing our back-up drive, was burglarized and the back-up drive, along with other items belonging to the employee, was stolen. Some information abogt present and former New Hampshire Dist ributors, LLC employees was stored on that drive. This information may have included your full name, home address, home and/or cell phone number, mail address, and Social Security number as well as files from your NHD, LLC laptop and /or desk top computers.

Attribution 1 Publication: NH AG's office Author:
Article Title: New Hampshire Distributors
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/nh-distributors-20160426.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-10	Pure Integration, LLC	VA	4/28/2016	Electronic	Business	Yes - Unknown #	Unknown

The incident involved an email from a 3rd party, impersonating our CEO and requesting a file of the 2015 W-2s. In response to that request all W-2s from 2015 were provided on April 14th. Subsequently, we determined that this email was a 3rd party phishing email. As you know, the W-2s include personally identifiable information such as name, social security number, address, and wages.

Attribution 1 Publication: NH AG's office Author:
Article Title: Pure Integration, LLC
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/pure-integration-20160428.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-09	Palm Beach County School District	FL	5/6/2016	Electronic	Educational	Yes - Published #	5,800

The teachers' Social Security numbers and names were inadvertently included in a file sent to an outside contractor, Educational Resource Strategies (ERS), as part of an ongoing budget review. ERS immediately took all necessary steps to purge the Social Security data from its system, and ensured that the Social Security data was not stored to any backup or storage system with ERS. The company provided an affidavit affirming the steps they took, as well as confirming the Social Security data was not used for any purpose or transmitted prior to deletion.

Attribution 1 Publication: databreaches.net Author:
Article Title: 5,800 Palm Beach County teachers notified of data security breach
Article URL: <http://www.databreaches.net/5800-palm-beach-county-teachers-notified-of-data-security-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-08	FDIC #1	DC	4/28/2016	Electronic	Government/Military	Yes - Published #	40,354

The security breach reported in the February 26th letter involved an FDIC employee who reportedly copied sensitive personally identifiable information or PII for over 10,000 individuals onto a portable storage device prior to separating from employment at the FDIC. Contrary to FDIC's representation to the Committee, this breach in fact effected "a total of 71,069 individuals and entities (consisting of 40,354 individuals and 30,715 banks and other entities)" In total, the employee stored over 100,000 files on the device. The Committee is very concerned that FDIC knowingly made gross misrepresentations regarding the disparity in the number of effected individuals and entities.

Attribution 1 Publication: GOP Interim Staff Report Author:
Article Title: FDIC #1
Article URL: <https://science.house.gov/sites/republicans.science.house.gov/files/documents/Final%20GOP%20Interim%20Staff%20>

Attribution 2 Publication: FEDERALTIMES.COM Author:
Article Title: Congress investigating October FDIC data breach
Article URL: <http://www.federaltimes.com/story/government/cybersecurity/2016/04/28/committee-investigating-fdic-breach/8361128>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-07	Ohio Department of Mental Health and Addiction Services	OH	5/9/2016	Electronic	Government/Military	Yes - Published #	59,000

Patients were sent a satisfaction survey by mail; however, the survey request was sent on postcards rather than in sealed envelopes. Consequently, the fact that each patient had received services related to mental health and addition was inadvertently exposed along with patients' names and addresses. Each year, OMHAS sends customer satisfaction surveys to patients to obtain feedback about the services they received.

Attribution 1 Publication: FEDERALTIMES.COM / hhs.com Author:
Article Title: Ohio Department of Mental Health and Addiction Services
Article URL: <http://mha.ohio.gov/Portals/0/assets/News/pressReleases/20160422-Media-Notice-Privacy-Breach.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-06	Nordic Consulting Partners / NavigateHCR	UT	5/5/2016	Electronic	Business	Yes - Published #	1,209

As explained in our April 22, 2016 e-mail, you have recently received a Form 1095-C (Employer-Provided Health Insurance Offer and Coverage). Nordic partnered with a vendor, NavigateHCR, to print and mail Form 1095-C to our employees and former employees. NavigateHCR's mailing partner determined that if the envelope holding the 1095-C form was shaken just right, the employee's social security number might have been visible. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / IN AG's Author:
Article Title: Nordic Consulting Partners / NavigateHCR
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Nordic%20Consulting%20Partners%20Inc%20SBN%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-05	Sanctuary Clothing	CA	5/3/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 22, 2016, we were advised by the company that maintains our e-commerce website that it had identified and removed a suspicious file. We quickly began an investigation and hired a third-party cybersecurity firm to assist us. Findings from the investigation show that if a visitor attempted to or did place an order on our website, www.sanctuaryclothing.com, from December 30, 2015 to March 22, 2016, information associated with the order being placed, including name, address, email address, payment card number, expiration date and security code (CVV), and, for customers who have a [Sanctuaryclothing.com](http://www.sanctuaryclothing.com) account, the username and password for their account, may have been obtained by an unauthorized third-party.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: Sanctuary Clothing
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Sanctuary%20Clothing%20LLC%20SBN%20to%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-04	CertifiKid	MD	3/19/2016	Electronic	Business	Yes - Published #	32,388

On March 25, 2016, CertifiKid discovered malicious software code that was inserted by unknown individuals into the server of its e-commerce website between the dates of January 25, 2016 and March 19, 2016. Subsequently, we determined that your personally identifiable information may be at risk. Our server houses our customer database. This database contains general user profile information including first and last name and some credit card information saved by some of our customers in their user profiles, including credit card number, credit card expiration date and card security code information. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: CertifiKid
Article URL: https://oag.ca.gov/system/files/CertifiKid%20Sample%20Consumer%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-03	Bay Area Children's Association	CA	5/6/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 1, 2016, we received notice from our electronic medical record provider that their electronic system was breached and some of our patient records were acquired by unauthorized persons. Specifically, they determined that cyber intruders may have installed malware in January 2015 and, through credential theft, accessed certain systems in their environment. We have been informed that the information accessed by unauthorized individuals may have included your name, address, telephone number, date of birth, social security number, medical insurance and health visit information if you provided such information to us.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: BAY AREA CHILDREN'S ASSOCIATION NOTIFIES PATIENTS OF PHI THEFT
Article URL: <http://www.hipaajournal.com/bay-area-childrens-association-notifies-patients-phi-theft-3420/>

Attribution 2 Publication: CA AG's office Author:
Article Title: Bay Area Children's Association
Article URL: https://oag.ca.gov/system/files/BACA%20Notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-02	Stonebridge Realty Advisors, Inc. / Xebec restaurant	CA	3/26/2016	Electronic	Business	Yes - Unknown #	Unknown

Based upon an extensive forensic investigation, it appears that unauthorized individuals installed malicious software on our payment processing systems that was designed to capture payment card information as it is inputted into those systems. Based on the information currently available from our investigation, we believe that the incident may have affected payment card data (including payment card account number and card expiration date) of individuals who used a payment card at our restaurant between November 8, 2015, and March 26, 2016.

Attribution 1 Publication: CA AG's office Author:
Article Title: Stonebridge Realty Advisors, Inc. / Xebec restaurant
Article URL: https://oag.ca.gov/system/files/49932072_6_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160509-01	Google	CA	5/9/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that a third-party vendor that provides Google with benefits management services mistakenly sent a document containing certain personal information of some of our Googlers to a benefits manager at another company. Promptly upon viewing the document, the benefits manager deleted it and notified Google's vendor of the issue. After the vendor informed us of the issue, we conducted an investigation to determine the facts.

Attribution 1 Publication: CA AG's office Author:
Article Title: Google
Article URL: https://oag.ca.gov/system/files/Google%20-%20Individual%20Notification%20Letter%20%28California%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160506-02	Kroger / Equifax W-2 Express	GA	5/6/2016	Electronic	Business	Yes - Published #	431,000

Identity thieves stole tax and salary data from big-three credit bureau Equifax Inc., according to a letter that grocery giant Kroger sent to all current and some former employees on Thursday. The nation's largest grocery chain by revenue appears to be one of several Equifax customers that were similarly victimized this year. Atlanta-based Equifax's W-2Express site makes electronic W-2 forms accessible for download for many companies, including Kroger — which employs more than 431,000 people. According to a letter Kroger sent to employees dated May 5, thieves were able to access W-2 data merely by entering at Equifax's portal the employee's default PIN code, which was nothing more than the last four digits of the employee's Social Security number and their four-digit birth year.

Attribution 1 Publication: Krebsonsecurity.com / OR AG's office Author: Brian Krebs
Article Title: Crooks Grab W-2s from Credit Bureau Equifax
Article URL: <http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160506-01	Colorado Department of Transportation	CO	5/5/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

"A probationary employee, who worked at CDOT from January 2016 to April 2016 and had access to confidential tax returns of DBE...firms, had been using personal information for improper purposes," the notification letter, sent Wednesday, said.

Attribution 1 Publication: denverpost.com Author:
Article Title: CDOT data breach may lead to identity theft, investigation ongoing
Article URL: http://www.denverpost.com/news/ci_29856130/cdot-data-breach-may-lead-identity-theft-investigation

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160505-05	Saint Agnes Medical Center	CA	5/2/2016	Electronic	Medical/Healthcare	Yes - Published #	2,812

Saint Agnes Medical Center was targeted by an isolated email phishing attack in which a scammer impersonated our Chief Executive Officer and requested that W-2 information be sent via email. There was no breach to any of our Saint Agnes systems and all patient information remains secure. Rather, we were the target of what is known as a BEC (Business Email Compromise/Correspondence) attack, which typically focuses on tax information that can be used to obtain fraudulent returns.

Attribution 1 Publication: CA AG's office Author:
Article Title: Saint Agnes Medical Center
Article URL: https://oag.ca.gov/system/files/SAMC%20Data%20Breach%20Notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160505-04	California State University Northridge	CA	5/4/2016	Electronic	Educational	Yes - Published #	70,265

On April 5, 2016, CSUN officials learned that online records containing information relating to CSUN Educational Opportunity Programs ("EOP") student applicants were potentially accessible online to outside parties. CSUN immediately began an investigation and discovered that an ID and password were mistakenly published on an internal-facing CSUN staff resources webpage that was visible to anyone with the specific website address, potentially allowing access to personal information of CSUN EOP applicants. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office / MD AG' Author:
Article Title: California State University Northridge
Article URL: https://oag.ca.gov/system/files/CSU_Adult_Notice_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160505-03	Hume Lake Christian Camps	CA	3/4/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 4, 2016, we discovered that between February 29, 2016 and March 4, 2016, as a result of a phishing incident, an unauthorized third party gained accessed to a Hume Lake employee's email account and, in turn, may have accessed files containing personal information.

Attribution 1 Publication: CA AG's office Author:
Article Title: Hume Lake Christian Camps
Article URL: https://oag.ca.gov/system/files/Hume%20Lake%20-%20CA%20Notice%20Letter_Redacted%20%286105565x7AB84%29

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160505-02	Pro Sports Daily	IL	4/8/2016	Electronic	Business	Yes - Unknown #	Unknown

We are writing to notify you that a breach of security of your personal information occurred on April 4, 2016. We learned that there was a hack into our database for the ProSportsDaily Forum website, which means that your account password to the ProSportsDaily Forum, despite encryption, may have been compromised.

Attribution 1 Publication: CA AG's office Author:
Article Title: Pro Sports Daily
Article URL: https://oag.ca.gov/system/files/Pro%20Sports%20Daily%20Security%20Breach%20Response%20Letter-Final_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160505-01	Lafler Moore Connerty & Webb	CA	4/5/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 8, 2016, we learned with a "high level of confidence" that information on our network was breached by an unauthorized individual starting on or about January 27, 2016, and who was potentially impacted.

Attribution 1 Publication: CA AG's office Author:
Article Title: Lafler Moore Connerty & Webb
Article URL: https://oag.ca.gov/system/files/Lafler%20AllClear%20letter%20Proof_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160504-03	Charles Schwab	CA	5/4/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We are contacting you to alert you to unusual login activity on your account(s), which began on or after March 25, 2016. We believe someone may have obtained your username and password from a non-Schwab account or website that you use and tried them successfully on Schwab.com. This type of account access can occur when you use the same username and password on multiple sites.

Attribution 1 Publication: CA AG's office / OR AG's office Author:
Article Title: Charles Schwab
Article URL: https://oag.ca.gov/system/files/Charles%20Schwab%20resubmitted%20May%202016_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160504-02	Office of Ken Waterman CPA PC	CA	5/3/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 30, 2016, KW learned that a possible security incident may have impacted the security of information stored on our servers. We immediately began an investigation and engaged independent, third-party forensic computer experts to assist. While the investigation is still ongoing, it appears that files stored on our system may have been accessed by an unauthorized individual. These files contain information related to your tax filings, and may have included your name, address, Social Security number, wage information, and in some instances bank account information.

Attribution 1 Publication: CA AG's office / MT AG's office Author:
Article Title: Office of Ken Waterman CPA PC
Article URL: https://oag.ca.gov/system/files/Ken%20Waterman%20CPA%20Notice%20Only_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160504-01	Areas	FL	4/29/2016	Electronic	Business	Yes - Published #	4,362

On April 29, 2016, Areas learned it was the target of an email phishing scheme which resulted in unauthorized access to your personal information. The personal information subject to this incident included name, address, and Social Security number. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: Areas
Article URL: https://oag.ca.gov/system/files/CA%20Sample%20Notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-19	YourEncore, Inc.	IN	3/21/2016	Electronic	Business	Yes - Unknown #	Unknown

The morning of March 7, 2016, W-2 tax form information for calendar year 2015 for current and former YourEncore employees was erroneously sent to an unauthorized third party via email. This was in response to a phishing email scam. This breach was not a compromise of enterprise systems.

Attribution 1 Publication: NH AG's office Author:
Article Title: YourEncore, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/your-encore-20160321.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 155 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-18	Union League Club of Chicago	IL	5/2/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 5, 2016, we learned that a Union League employee was using keylogging software on certain Union League computers without authorization. Upon learning of the employee's use of the software, we promptly began an investigation, including retaining an expert computer security firm to examine Union League computers. Through the investigation, we determined that the employee used the keylogger software to obtain information entered into certain Union League computers, including payment card information regarding payments made by some of our guests.

Attribution 1 Publication: NH AG's office Author:
Article Title: Union League of Chicago
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/union-league-20160429.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-17	Tiger Leasing	NY	4/29/2016	Electronic	Business	Yes - Unknown #	Unknown

We are contacting you regarding a data security Incident that occurred sometime between April 9, 2016 and April 14, 2016. Credentials assigned to Tiger Leasing were used without authorization to access credit information from a consumer information provider.

Attribution 1 Publication: NH AG's office Author:
Article Title: Tiger Leasing
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/tiger-leasing-20160429.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-16	Smith & Nephew PLC (Blue Belt Technologies)	MN	3/24/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Yesterday, March 23, 2016, Smith & Nephew was notified that on Monday, March 21, 2016, Blue Belt's former third-party payroll vendor, Dare Enterprises, was the victim of a fraudulent scheme which resulted in the mistaken release of employee W2 forms for the year ending December 31, 2015. The personal information involved included the first and last name, home address, and Social Security number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Smith & Nephew PLC (Blue Belt Technologies)
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/smith-nephew-20160324.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-15	MMF Industries (Block and Company, Inc.)	MI	3/31/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 21, 2016, we discovered that malicious code had been placed on our web server on or about February 9, 2016. Although our investigation is ongoing, we believe that the malware may have targeted your personal information, including your first and last name, billing or mailing address, email address, and credit card information (card holder name, credit card account number, expiration month and year, and card security code).

Attribution 1 Publication: NH AG's office / MT AG's office Author:
Article Title: MMF Industries (Block and Company, Inc.)
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/mmf-industries-20160331.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-14	Home for Little Wanderers	MA	4/25/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 11, 2016, we discovered that our company was targeted in an email spoofing attack. Through this attack, a request was made for 2015 IRS Tax Form W-2 information. Unfortunately, a report with some information was emailed before it was discovered that the request was made from a fraudulent account by an individual purporting to be me.

Attribution 1 Publication: NH AG's office Author:
Article Title: Home for Little Wanderers
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/home-little-wanderers-20160425.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 156 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-13	Hi-Tec	CA	4/29/2016	Electronic	Business	Yes - Published #	1,603

Hi-Tec received reports from several customers of fraudulent charges appearing on their payment cards shortly after they were used to make a purchase on our Magnum Boots online order page. Hi-Tec immediately began working with the company that developed and maintains its websites. On March 11, 2016, the web developer reported that it had identified unauthorized code that had been inserted into the program that operates its order completion page. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: Hi-Tec
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/hi-tec-20160429.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-12	HAECO Americas	NC	4/29/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 15, 2016, we became aware that HAECO Americas was the target of a phishing email in March 2016 that resulted in the unauthorized acquisition by a third party of certain employee information. The employee information was contained in W-2 forms, and included names, addresses, Social Security numbers, and wage and tax information.

Attribution 1 Publication: NH AG's office Author:
Article Title: HAECO Americas
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/haeco-americas-20160429.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-11	Draper James	TN	4/26/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 24, 2016, we were made aware of vulnerability in the security of the www.draperjames.com checkout pages that affected a small fraction of Draper James' customers. Upon discovery and with the assistance of our website platform manager, we immediately ensured the vulnerability was remedied and launched an investigation.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Draper James
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/draper-james-20160426.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-10	Avendra, LLC	MD	3/23/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 7, 2016, my client became aware that certain 2015 payroll data was acquired by an unauthorized party on or about March 7, as a result of a phishing attack targeted at Avendra. The 2015 payroll data contained the IRS Form W-2s, including name, address, Social Security number, and 2015 salary and tax information, for one New Hampshire resident.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Avendra, LLC
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/avendra-20160323.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-09	Meeting Street School	RI	4/13/2016	Electronic	Educational	Yes - Unknown #	Unknown

Meeting Street School says they were victims of a phishing scheme last month. The school reportedly received seemingly legitimate emails that were probing for personal information.

Attribution 1 Publication: wpri.com Author:
Article Title: Meeting Street School hit by identity theft scheme
Article URL: <http://wpri.com/2016/04/13/meeting-street-school-hit-by-identity-theft-scheme/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-08	Brunswick School District	ME	3/31/2016	Electronic	Educational	Yes - Unknown #	Unknown

An employee in the Brunswick School Department's administrative office Monday responded to what turned out to be a phishing scam, emailing to the scammer tax forms, minus dates of birth and Social Security numbers, from about 400 school department employees.

Attribution 1 Publication: bangordailynews.com Author:
Article Title: Maine school employees' tax info sent to email scammer
Article URL: <http://bangordailynews.com/2016/03/31/news/midcoast/maine-school-employees-tax-info-sent-to-email-scammer/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-07	Allegheny College	PA	4/30/2016	Electronic	Educational	Yes - Unknown #	Unknown

At least 74 non-student employees of Allegheny College have recently experienced personal information theft, including having their Social Security numbers accessed. The college believes the information was accessed through the hacking of Automatic Data Processing, Inc., according to an email sent out by Rick Holmgren, vice president for Information Services and Assessment, to all regular employees. More specifically, Holmgren said the college suspects hackers accessed the information through ADP's iPay program, which allows enrolled employees to access their paystubs, W-2s and Forms 1099 electronically.

Attribution 1 Publication: databreaches.net / alleghenycampus.co Author:
Article Title: Campus payroll service hacked
Article URL: <http://alleghenycampus.com/13219/news/campus-payroll-service-hacked/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-06	Florida Hospital Medical Group	FL	5/2/2016	Electronic	Medical/Healthcare	Yes - Published #	1,906

The medical group, which is the physician practice arm of Florida Hospital, said on Friday that a transcription services company had used an unencrypted email account to sent some patient medical records back to doctors' offices. The e-mails included names, birth dates, medications and other information regarding patients' medical history.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Florida Hospital Medical Group notifies patients after transcription service error
Article URL: <http://www.databreaches.net/florida-hospital-medical-group-notifies-patients-after-transcription-service-error/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-05	Alpha Payroll Services, LLC	PA	5/2/2016	Electronic	Business	Yes - Unknown #	Unknown

On or about March 1 or 2, an Alpha Payroll employee responded to a "phishing" scam email in which the sender represented himself or herself to be the CEO of Alpha Payroll and disguised his or her email address as that of the CEO. In this email, the fraudster requested copies of all the 2015 W-2 forms produced by Alpha Payroll on behalf of its customers.

Attribution 1 Publication: databreaches.net / dailydot.com / VT AG Author:
Article Title: Phishing scam hits payroll company, exposing all clients' W-2 data to criminals
Article URL: <http://www.dailydot.com/politics/alpha-payroll-services-phishing-scam-w2-clients/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-04	Brunswick Corporation / Mercury Marine	IL	5/2/2016	Electronic	Business	Yes - Published #	13,000

Brunswick Corporation today reported it has been the victim of an email phishing incident that resulted in the potential unauthorized disclosure of 2015 W-2 information of a large number of current and former employees.

Attribution 1 Publication: databreaches.net / Brunswick statement Author:
Article Title: Large number of Brunswick Corporation employees being notified of W-2 data breach
Article URL: <http://www.databreaches.net/large-number-of-brunswick-corporation-employees-being-notified-of-w-2-data-breach/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 158 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-03	EqualizeRCM Services	TX	5/3/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On February 29, EqualizeRCM learned that a laptop had been stolen from an employee on February 25 or 26. A notification letter, signed by Janine Anthony Bowen of LeClairRyan to the New Hampshire Attorney General's Office, does not indicate whether the laptop was stolen from the employee's home, a car, or some other location.

Attribution 1 Publication: databreaches.net / NH AG's office / MT Author:
Article Title: Stolen billing vendor's laptop held patient info from 8 medical facilities
Article URL: <http://www.databreaches.net/stolen-billing-vendors-laptop-held-patient-info-from-8-medical-facilities/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-02	South Loop CPA	IL	4/29/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 5, 2016, a password-protected laptop computer belonging to South Loop was stolen from our offices. As soon as we discovered the theft, we notified law enforcement and we are cooperating with their investigation. We also conducted an investigation to determine what information, specifically, was stored on the laptop. From our investigation, it appears the files may have included your tax returns, which include your name, address, Social Security number, bank account number, and wage information.

Attribution 1 Publication: VT AG's office Author:
Article Title: South Loop CPA
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/South%20Loop%20CPA%20SBN%20to%20Consumers.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160503-01	ProSchools / QuickCert	OR	4/29/2016	Electronic	Educational	Yes - Unknown #	Unknown

If you accessed ProSchools.com between February 4, 2016 and March 16, 2016, the malicious software (also known as "mal ware" or "script") that attacked our system may have tried to copy your name, mailing address, email address, phone number and credit card information (including CVV number).

Attribution 1 Publication: OR AG's office / NH AG's office / MD A Author:
Article Title: ProSchools / QuickCert
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/601388157>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160502-01	Solano Community College	CA	5/2/2016	Electronic	Educational	Yes - Published #	1,206

Solano Community College in Fairfield, Calif., was hit with a spearphishing attack led to the W-2 information for about 1,200 staffers being compromised.

Attribution 1 Publication: Scmagazine.com / CA AG's office Author: Doug Olenick
Article Title: 1,206 Solano Community College employees victimized in W-2 data breach
Article URL: <http://www.scmagazine.com/1206-solano-community-college-employees-victimized-in-w-2-data-breach/article/493732/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-12	University of the Southwest	NM	4/21/2016	Electronic	Educational	Yes - Unknown #	Unknown

USW uses a third-party vendor to host its employee W-2 and wage information. On February 2, 2016, USW learned that unauthorized access to certain current and former employee W-2s stored on the third-party vendor's portal may have occurred.

Attribution 1 Publication: NH AG's office Author:
Article Title: University of the Southwest
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/university-southwest-20160422.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 159 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-11	TTI Floor Care North America	OH	4/14/2016	Electronic	Business	Yes - Unknown #	Unknown

In October and November of 2015, TTI Floor Care North America ("TTI") received notification from six (6) customers informing us that shortly after placing an order with our customer service center, the credit cards they used for payment was used to make unauthorized purchases from various locations. TTI promptly launched an investigation into this matter and discovered that a single employee had taken the orders from these customers whose credit cards were compromised.

Attribution 1 Publication: NH AG's office / MT AG's office Author:
Article Title: TTI Floor Care North America
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/tti-floor-care-20160414.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-10	Gryphon Technologies, LC	DC	3/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On Monday, March 7, Gryphon discovered that it was the targeted victim of two email spoofing attacks by individuals purporting to be the company's CEO and CFO. Through these attacks, two separate requests were made between February 29, 2016 and March 7, 2016 from what appeared to be legitimate Gryphon email addresses for all 2015 employee W2 information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Gryphon Technologies, LC
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/gryphon-technologies-20160321.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-09	BloomReach, Inc.	CA	4/19/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 11, 2016, your W-2 information was disclosed to an unauthorized individual as part of a phishing attack. We discovered the disclosure on April 11, 2016. The W-2 information included your name, address, social security number, wages, and withholdings.

Attribution 1 Publication: NH AG's office Author:
Article Title: BloomReach, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/bloomreach-20160419.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-08	Vail Valley	CO	4/27/2016	Electronic	Medical/Healthcare	Yes - Published #	3,118

A physical therapist formerly employed at Howard Head Sports Medicine was discovered to have copied the PHI of patients and taken the data to his new employer. Prior to leaving employment, the physical therapist downloaded patient PHI onto a USB drive on two separate occasions.

Attribution 1 Publication: hippajournal.com Author:
Article Title: VAIL VALLEY MEDICAL CENTER NOTIFIES 3,118 PATIENTS OF UNAUTHORIZED PHI DISCLOSURE
Article URL: <http://www.hippajournal.com/vail-valley-medical-center-notifies-3118-patients-unauthorized-phi-disclosure-3406/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-07	American Dental Association (ADA)	IL	4/28/2016	Electronic	Business	Yes - Unknown #	Unknown

The American Dental Association (ADA) says it may have inadvertently mailed malware-laced USB thumb drives to thousands of dental offices nationwide.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Dental Assn Mails Malware to Members
Article URL: <http://krebsonsecurity.com/2016/04/dental-assn-mails-malware-to-members/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 160 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-06	Bryant & Stratton College	NY	4/25/2016	Electronic	Educational	Yes - Unknown #	Unknown

On March 10, 2016, an email was sent to two Bryant & Stratton students, which inadvertently attached a file containing your personally identifiable information ("PII"), including name, Student ID number and social security number, and information about financial aid references.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Bryant & Stratton College
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Bryant%20%26%20Stratton%20College%20SBN%20to%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-05	Michels Corporation	WI	4/26/2016	Electronic	Business	Yes - Published #	8,161

On April 16, 2016, a Michels employee was targeted by an isolated email phishing scam in which an individual outside of Michels impersonated a Michels executive requesting certain information for Michels employees. The result of the cyber scam was that certain information related to current and former employees who would have received a W-2 for 2015 was disclosed. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / IN AG's office Author:
 Article Title: Michels Corporation
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Michels%20Corporation%20SBN%20to%20Consumers.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-04	GoldKey/PHR	VA	4/25/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 3, 2016 we discovered that on February 29, 2016, as a result of a criminal phishing email, an unauthorized third party may have obtained an electronic file containing Form W-2s for each associate. Form W-2s contain certain personal information on each associate employed in 2015.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
 Article Title: GoldKey/PHR
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/GoldKey%20PHR%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-03	Geltrude & Company, LLC	NJ	4/15/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 17, 2016, we discovered that our company (was) the victim of a cyberattack on our computer system. Through this attack, an unknown individual or individuals was able to access our computer system and files containing information on our clients.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Geltrude & Company, LLC
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Geltrude%20%26%20Company%20SBN%20to%20Consu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-02	Advance International Marketing (AIM)	NC	4/4/2016	Electronic	Business	Yes - Published #	63,888

AIM Inc received a report on April 4, 2016, that an unauthorized person was able to gain access to certain images that had been uploaded to our website. We immediately conducted an investigation, engaged a leading security firm, and alerted law enforcement. The investigation determined that the unauthorized person identified an issue in the document upload feature of the website that customers used to upload fireanns license and documents for age verification. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
 Article Title: Advance International Marketing
 Article URL: https://oag.ca.gov/system/files/CA_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 161 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160429-01	LuckyPet	WA	4/29/2016	Electronic	Business	Yes - Published #	11,333

On approximately October 12, 2015, an unknown and unauthorized party exploited a vulnerability in the third-party shopping cart software used on our Web site .and inserted malicious software that intercepted information provided by customers while making a purchase. Your name, address, and credit card information (including expiration date and security code) were among the information potentially intercepted. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: LuckyPet
Article URL: https://oag.ca.gov/system/files/%23130774091%2C%20v1%20_LEGAL_%20-%20LuckyPet%20Multistate%20Notificatio

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160427-01	BeautifulPeople	NY	4/27/2016	Electronic	Business	Yes - Unknown #	Unknown

A data breach at the online dating site BeautifulPeople.com has exposed over a million members' account information, including personal details such as sexual orientation, marital status, income, birth date, email address and home address.

Attribution 1 Publication: naked security by sophos Author: John Zorabedian
Article Title: Dating site that once faked being hacked is breached for real this time
Article URL: <https://nakedsecurity.sophos.com/2016/04/27/dating-site-that-once-faked-being-hacked-is-breached-for-real-this-time/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-14	Trinity Heating & Air, Inc. dba Trinity Solar	NJ	4/12/2016	Electronic	Business	Yes - Published #	1,156

On Tuesday, April 5th, 2016, Trinity Solar, learned that on March 11, 2016, an employee sent 1,156 employee W-2's to an e-mail account that appeared to belong to a company executive, but was in fact an unauthorized outside party. Of these 1,156 employees, 5 reside in New Hampshire. It is believed that the imposter requested the W -2 forms and the employee complied with what she believed to be an authentic request from a superior.

Attribution 1 Publication: NH AG's office Author:
Article Title: Trinity Heating & Air, Inc. dba Trinity Solar
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/trinity-heating-20160412.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-13	TD Bank	NJ	4/4/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently learned that on March 24, 2016, a document containing some of your personal information was inadvertently sent to an incorrect email address and was received by an unauthorized party not associated with TD Bank. The personal information they may have received included your name, address, Social Security number, and date of birth.

Attribution 1 Publication: NH AG's office Author:
Article Title: TD Bank
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/td-bank-20160331.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-12	Seven Hills Foundation	MA	4/15/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

We are writing to inform you that a copy of your W2 form, which includes your name, address, social security number and wage and withholdings information, was obtained by an unknown and unauthorized person or persons on Friday April 8, 2016. This incident does not impact employees of Seven Hills Rhode Island, Stetson School, Seven Hills Pediatric Centers and some Respite employees.

Attribution 1 Publication: NH AG's office Author:
Article Title: Seven Hills Foundation
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/seven-hills-foundation-20160415.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-11	NetBrain Technologies, Inc.	MA	4/20/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 3, 2016, an unauthorized person or person(s) posing as a senior NetBrain executive emailed a more junior NetBrain employee requesting copies of all 2015 W -2 forms. The employee replied to the email, attaching the requested documents. Very shortly after the reply email was sent, NetBrain learned that the email was a scam and that the electronic W -2 forms were fraudulently obtained by an unauthorized party.

Attribution 1 Publication: NH AG's office / VT AG's office Author:
Article Title: NetBrain Technologies, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/netbrain-technologies-20160420.PDF>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-10	Mountain Park Health Center	AZ	4/15/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On March 22, 2016, MPHIC's administrative offices, and some locked file cabinets where employee personnel files were secured, were broken into. Although the file cabinets were opened and it appears that the burglars rittled through the drawers, none of the contents of the filing cabinet were stolen. MPHIC immediately began an investigation to detemtime what information was in the tile cabinets and determined that it contained employee personnel files.

Attribution 1 Publication: NH AG's office / databreaches.net Author:
Article Title: Mountain Park Health Center
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/mountain-park-health-20160415.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-09	Landstar System, Inc.	FL	3/21/2016	Electronic	Business	Yes - Published #	1,362

On Friday, March 18, 2016, Landstar System, Inc. (collectively with its subsidiaries and affiliates, "Landstar") learned that it suffered a phishing attack, which resulted in the unauthorized disclosure of employees' 2015 W-2 Forms. In conducting an internal investigation ofthis incident, Landstar discovered that a similar phishing incident also occurred on February 24, 2016, which also resulted in the unauthorized disclosure of employees' 2015 W-2 Forms. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: Landstar System, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/landstar-system-20160321.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-08	Eastern Benefits Group	MA	4/21/2016	Electronic	Business	Yes - Unknown #	Unknown

We discovered in early April2016 that tax documents of employees at Lawton Welding Company, Inc. mailed on March 31 , 2016 may have been received by other employees in error. The personal information included your name, postal address, Social Security number and insurance premium amounts.

Attribution 1 Publication: NH AG's office Author:
Article Title: Eastern Benefits Group
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/eastern-bank-20160421.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-07	Client Network Services, Inc.	MD	4/21/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently discovered that our company was the victim of an email spoofing attack by an individual purporting to be our CEO. Through this attack, a request was made from what appeared to be a legitimate CNSI email address for 2015 employee W2 information. Unfortunately this information was provided before we discovered that the request was fraudulent. We discovered the fraudulent nature of this request on Wednesday, March 23, and have been working to investigate and to mitigate the impact of the attacks.

Attribution 1 Publication: NH AG's office Author:
Article Title: Client Network Services, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/client-network-20160418.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-06	Behavioral Science Technology	CA	4/22/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 19, 2016, an unauthorized individual, impersonating a BST executive, contacted a BST employee to request certain information about BST employees. Before it was determined that the request was fraudulent, an electronic file was provided, which contained information about the affected employees. Fortunately, the file was password protected, and the password was not sent to the unauthorized individual.

Attribution 1 Publication: NH AG's office Author:
Article Title: Behavioral Science Technology
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/behavioral-science-20160422.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-05	Agenus	MA	4/19/2016	Electronic	Business	Yes - Unknown #	Unknown

An unknown entity used a spear phishing technique to obtain personal information about Agenus' employees by inducing one employee to send certain employee W-2 forms to the entity under false pretense.

Attribution 1 Publication: NH AG's office Author:
Article Title: Agenus
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/agenus-20160419.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-04	Fruitful Yield	IL	4/21/2016	Electronic	Business	Yes - Published #	3,921

It recently came to Fruitful Yield's attention through an outside service provider for these websites that during the time period from January 7, 2016 to March 21, 2016, an unauthorized user gained access to the sites and may have acquired certain information about Fruitful Yield customers. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's Office / IN AG's office Author:
Article Title: Fruitful Yield
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/fruitful-yield-20160420.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-03	Spotify	CA	4/25/2016	Electronic	Business	Yes - Unknown #	Unknown

A list containing hundreds of Spotify account credentials – including emails, usernames, passwords, account type and other details – has popped up on the website Pastebin, in what appears to be a possible security breach. After reaching out to a random sampling of the victims via email, we've confirmed that these users' Spotify accounts were compromised only days ago. However, Spotify says that it "has not been hacked" and its "user records are secure."

Attribution 1 Publication: Techcrunch.com Author:
Article Title: Hundreds of Spotify credentials appear online – users report accounts hacked, emails changed
Article URL: <http://techcrunch.com/2016/04/25/hundreds-of-spotify-credentials-appear-online-users-report-accounts-hacked-emails>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-02	Akron General Edwin Shaw Rehabilitation	OH	4/26/2016	Electronic	Medical/Healthcare	Yes - Published #	975

On February 24, 2016, Edwin Shaw Rehab leadership became aware that a "flash" drive device containing limited protected health information belonging to some patients who received services in 2010 or 2011 had been inadvertently misplaced or disposed of at a February 19, 2016, business-related event, which was closed to the general public.

Attribution 1 Publication: databreaches.net / hospital notice Author:
Article Title: Edwin Shaw employee loses unencrypted flash drive with 975 patients' info
Article URL: <http://www.databreaches.net/edwin-shaw-employee-loses-unencrypted-flash-drive-with-975-patients-info/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 164 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160426-01	Berkeley Public Schools	CA	4/21/2016	Electronic	Educational	Yes - Unknown #	Unknown

The Bay Area News Group, a publisher of multiple Bay Area newspapers, annually conducts surveys of all public agencies in the Bay Area regarding employee salary and related payroll information. They are entitled to this information pursuant to the California Public Records Act. The District compiled the requested information and transmitted it in an electronic file last week to the reporter who was coordinating the collection of the data. Unfortunately, the District inadvertently sent an electronic file that contained social security numbers.

Attribution 1 Publication: CA AG's office Author:
Article Title: Berkeley Public Schools
Article URL: https://oag.ca.gov/system/files/BerkeleyUSD-NotificationBANG-sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-15	TMEIC Corporation	VA	4/18/2016	Electronic	Business	Yes - Published #	300

In particular, in March 2016 a TMEIC employee fell victim to a fraudulent email phishing scheme requesting W-2 wage information. The TMEIC employee sent the W-2 information of TMEIC's employees (approximately 300 individuals) to the fraudulent email. One of the impacted employees is a New Hampshire resident.

Attribution 1 Publication: Databreaches.net / NH AG's office Author:
Article Title: TMEIC Corporation
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/tmeic-20160418.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-14	Wynden Stark, dba GQR Global Markets/City	NY	4/5/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 1, 2016, due to a fraudulent communication to us by someone posing as our managing director (often referred to as a "phishing" or "spoofing" incident), an error was made and your federal W-2 form was sent to an unknown third party. The W-2 form included information relating to your employment, including your name, address, social security number and 2015 wages and tax withholding information.

Attribution 1 Publication: databreaches.net / justice.oregon.gov Author:
Article Title: Wynden Stark, dba GQR Global Markets/City Internships
Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1291171884>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-13	OpSec	PA	3/25/2016	Electronic	Business	Yes - Unknown #	Unknown

In early March, "hackers accessed an email containing an attachment which included 2015 W-2 tax forms for all salaried and hourly employees, including some former employees," reads an email sent to people working for OpSec Security.

Attribution 1 Publication: databreaches.net / lancasteronline.com Author: Tim Stuhldreher
Article Title: Hackers reportedly access OpSec employee data
Article URL: http://lancasteronline.com/business/local_business/hackers-reportedly-access-opsec-employee-data/article_66545416

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-12	Morongo Casino	CA	4/15/2016	Electronic	Business	Yes - Unknown #	Unknown

Morongo Casino employees have been told they are victims of a "cybercrime" after someone nabbed their 2015 W-2 tax information, including names and Social Security numbers, a spokesman confirmed Friday.

Attribution 1 Publication: databreaches.net / redlandsdailyfacts.co Author:
Article Title: Morongo Casino employees' W-2 information hacked
Article URL: <http://www.redlandsdailyfacts.com/technology/20160415/morongo-casino-employees-w-2-information-hacked>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 165 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-11	DealerSocket, Inc.	CA	4/18/2016	Electronic	Business	Yes - Published #	1,350

On April 11, 2016, DealerSocket was the target of a phishing email scheme that purported to be from a DealerSocket executive leader and requested personal information about employees. The information involved included the personal information found in your W-2, including your: (i) full name; (ii) home address; (iii) social security number; and (iv) 2015 earnings as a DealerSocket employee. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / databreaches.net / IN A Author:
Article Title: DealerSocket, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/dealersocket-20160418.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-10	General Fasteners Company (MNP)	MI	4/6/2016	Electronic	Business	Yes - Published #	1,505

General Fasteners Company recently discovered that an electronic file containing personal information was disclosed to a third party. The Company's investigation of the incident indicates that your completed W-2 tax form for 2015 was included in that file. The file was disclosed to the third party on March 6, 2016, and the Company discovered the issue on the same day. (Consumers affected per IN AG's office)

Attribution 1 Publication: databreaches.net / NH AG's office / IN A Author:
Article Title: General Fasteners Company (MNP)
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/mnp-20160406.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-09	Hutchinson Community College	KS	4/6/2016	Electronic	Educational	Yes - Published #	1,357

The W2 information of 1,357 employees at Hutchinson Community College was leaked to an unauthorized email address.

Attribution 1 Publication: databreaches.net / KSNT.com Author: Molly Brewer
Article Title: Data leak at Hutchinson Community College
Article URL: <http://ksnt.com/2016/04/06/data-leak-at-hutchinson-community-college/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-08	BackOffice Associates	MA	4/17/2016	Electronic	Business	Yes - Unknown #	Unknown

The company told employees via email Monday that "tax documentation" — specifically the 2015 W-2s of its United States-based employees — was "inadvertently disclosed to an unknown individual." The information included first and last names, home addresses, social security numbers and 2015 compensation data. The email, which was sent to the Times and confirmed by several BackOffice employees, said a preliminary investigation indicated the disclosure apparently happened on March 18 but the company did not find out until

Attribution 1 Publication: databreaches.net / capecodtimes.com Author: Lorelei Stevens
Article Title: BackOffice Associates warns staff of breach
Article URL: <http://www.capecodtimes.com/article/20160417/NEWS/160419567>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-07	Ash Brokerage Firm	IN	4/7/2016	Electronic	Banking/Credit/Financial	Yes - Published #	423

As far as company executives have been able to determine, the information in W-2 forms for 423 people — a combination of current workers and former workers — were delivered to a third party. The scam worked because the fraudulent email, requesting the W-2 data, arrived looking as if it came from an Ash Brokerage employee using an Ash email address. Instead of being routed to that employee, the W-2 information was delivered to an email address that so far has proved untraceable, Grover said.

Attribution 1 Publication: news-sentinel.com / databreaches.net Author: Bob Caylor
Article Title: Personal tax data of more than 400 Ash
Article URL: <http://www.news-sentinel.com/news/local/Personal-tax-data-of-more-than-400-Ash-Brokerage-workers-taken-in-phishi>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-06	Bowdoin College	ME	4/1/2016	Electronic	Educational	Yes - Published #	275

Bowdoin College officials on Thursday notified 275 current and former faculty and staff members that their Social Security numbers, addresses and other personal information was accessed improperly through the company that manages the college's payroll tax filings. Officials from the Maine Revenue Service contacted Bowdoin on Tuesday to say the MRS had received a suspicious tax return that received valid W-2 information, Bowdoin spokesman Scott Hood said Friday. The data theft was discovered one day after an employee in the Brunswick School Department's administrative office responded to what turned out to be a phishing scam and emailed to the scammer tax forms minus dates of birth and Social Security numbers for about 400 school department employees.

Attribution 1 Publication: [bangordailynews.com / databreaches.ne](#) Author:
 Article Title: Hacker steals tax information of 275 current, former Bowdoin employees
 Article URL: <https://bangordailynews.com/2016/04/01/news/midcoast/hacker-steals-tax-information-of-275-current-former-bowdoin->

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-05	Kaiser Permanente - Inland Empire	CA	4/23/2016	Electronic	Medical/Healthcare	Yes - Published #	2,451

A mail delivery truck carrying the personal information of 2,400 Kaiser Permanente members on the Inland Empire Health Plan was stolen last month from a parking lot in Santa Clarita, officials announced Friday. The mail delivery truck contained "Evidence of Coverage" handbooks for Kaiser Permanente California Medi-Cal members in Southern California who are part of the Inland Empire Health Plan. It was not parked in a secure area, which violated Kaiser's vendor mail delivery policies, officials said in a news release. The stolen property contained protected health information, including names, addresses and the handbooks, which provide a generic overview of plan benefits.

Attribution 1 Publication: [Press Enterprise / beckershospitalreview](#) Author: Nereida Moreno
 Article Title: HEALTHCARE: 2,400 members' info stolen, Kaiser Permanente says
 Article URL: <http://www.pe.com/articles/permanente-800852-kaiser-members.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-04	Grand Sierra Resort / (MEI-GSR)	NV	4/25/2016	Electronic	Business	Yes - Published #	156,508

On or around September 29, 2015, the Grand Sierra Resort was contacted by law enforcement regarding an investigation into a potential compromise of payment card information used at food and retail locations at the Grand Sierra Resort. We immediately began to cooperate with law enforcement and to investigate this matter. Third party forensics investigators were retained to assist the Grand Sierra Resort. On or around January 11, 2016, these investigators confirmed that certain guest payment card information for cards used at food and retail locations at the Grand Sierra Resort may have been compromised. (MEI-GSR)

Attribution 1 Publication: [databreaches.net / GSR website / IN AG](#) Author:
 Article Title: Grand Sierra Resort guest payment cards breached in 2014 and again in 2015
 Article URL: <http://www.databreaches.net/grand-sierra-resort-guest-payment-cards-breached-in-2014-and-again-in-2015/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-03	RMA Medical Centers of Florida	FL	4/7/2016	Electronic	Medical/Healthcare	Yes - Published #	3,906

RMA Medical Centers of Florida FL Healthcare Provider 3906 04/07/2016 Theft Laptop

Attribution 1 Publication: [hhs.gov](#) Author:
 Article Title: RMA Medical Centers of Florida
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-02	Sacred Heart Health System, Inc.	FL	4/12/2016	Electronic	Medical/Healthcare	Yes - Published #	532

Sacred Heart Health System, Inc FL Healthcare Provider 532 04/12/2016 Unauthorized Access/Disclosure Other

Attribution 1 Publication: [hhs.gov](#) Author:
 Article Title: Sacred Heart Health System, Inc.
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 167 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160425-01	American Fidelity Assurance Company	OK	4/13/2016	Paper Data	Medical/Healthcare	Yes - Published #	2,664

On February 15, 2016, debit card substantiation letters were mailed to some of our Customers. An error in the mailing process caused some of our Customers to receive information that was intended for a different Customer. This means that a portion of one Customer's letter may have been inadvertently mailed to another Customer.

Attribution 1 Publication: [hhs.gov / databreaches.net / americanfid](http://hhs.gov/databreaches.net/americanfid) Author:
Article Title: American Fidelity Assurance Company
Article URL: <https://americanfidelity.com/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-12	Wyoming Medical Center	WY	4/21/2016	Electronic	Medical/Healthcare	Yes - Published #	3,184

On Feb. 25, an unidentified third party had access for 15 minutes to two Wyoming Medical Center email accounts containing patient records, the Casper hospital said in a statement. The records contained patient names, medical record numbers, account numbers, dates of hospital service, birth dates and some medical information, the statement said. Patients' addresses, Social Security numbers or insurance information were not in the records.

Attribution 1 Publication: [databreaches.net / WMC comment](http://databreaches.net/WMCcomment) Author:
Article Title: Wyoming Medical Center reports patient record breach
Article URL: <http://www.databreaches.net/wyoming-medical-center-reports-patient-record-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-11	Voya Financial Advisors, Inc.	NY	4/13/2016	Electronic	Business	Yes - Unknown #	Unknown

Perpetrators used your financial advisor's personal information to gain unauthorized access to VFA's systems, including [INSERT NAME]'s client records. VFA was able to detect and remediate the unauthorized access within a matter of hours, but it is possible that the perpetrator viewed your personal information while in the system.

Attribution 1 Publication: CA AG's office Author:
Article Title: Voya Financial Advisors, Inc.
Article URL: <https://oag.ca.gov/system/files/VFA%20Fraud%20Case%20Individual%20Notification%20Letter%20CA%20284-20-16>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-10	UFC Gym	CA	4/12/2016	Electronic	Business	Yes - Unknown #	Unknown

On April 4, 2016 we had several computers stolen from our corporate office in Santa Ana, California. Some of the computers that were stolen from our office contained certain company payroll data which may have included your personal information such as your W-2 forms and/or other documents that contained your name, address, birthdate and social security number

Attribution 1 Publication: CA AG's office Author:
Article Title: UFC Gym
Article URL: https://oag.ca.gov/system/files/Data%20Breach%20Notice%20California%20Form_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-09	Vibrant Body Wellness	CA	3/11/2016	Electronic	Medical/Healthcare	Yes - Published #	726

A chiropractic office is urging its patients to get in touch, as well as contact credit reporting agencies and take precautions against unauthorized use of their personal data, following a break-in last month. Vibrant Body Wellness was burgled over the weekend of March 5, the company announced on its website (vibrantbodywellness.com) and in a news release Friday. Stolen items include a laptop and a backup hard drive.

Attribution 1 Publication: [hhs.gov / eastbaytimes.com](http://hhs.gov/eastbaytimes.com) Author:
Article Title: Vibrant Body Wellness
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 168 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-08	Sisters of Charity of Leavenworth Health System	CO	4/5/2016	Paper Data	Medical/Healthcare	Yes - Published #	540
Sisters of Charity of Leavenworth Health System Health Benefits Plan CO Business Associate 540 04/05/2016 Unauthorized Access/Disclosure Paper/Films							

Attribution 1 Publication: [hhs.gov](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) Author:
 Article Title: Sisters of Charity of Leavenworth Health System Health Benefits Plan
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-07	BioReference Laboratories, Inc.	NJ	4/8/2016	Electronic	Medical/Healthcare	Yes - Published #	3,563
BioReference Laboratories, Inc NJ Healthcare Provider 3563 04/08/2016 Unauthorized Access/Disclosure Other							

Attribution 1 Publication: [hhs.gov](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) Author:
 Article Title: BioReference Laboratories, Inc.
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-06	Target Corporation Health Plan	MN	4/5/2016	Paper Data	Medical/Healthcare	Yes - Published #	719
Target Corporation Health Plan MN Business Associate 719 04/05/2016 Unauthorized Access/Disclosure Paper/Films							

Attribution 1 Publication: [hhs.gov](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) Author:
 Article Title: Target Corporation Health Plan
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-05	Pacific Gas and Electric Company	CA	4/5/2016	Paper Data	Business	Yes - Published #	2,426
Pacific Gas and Electric Company CA Business Associate 2426 04/05/2016 Unauthorized Access/Disclosure Paper/Films							

Attribution 1 Publication: [hhs.gov](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) Author:
 Article Title: Pacific Gas and Electric Company
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-04	United Community & Family Services	CT	4/12/2016	Electronic	Medical/Healthcare	Yes - Published #	1,000
United Community & Family Services CT Healthcare Provider 1000 04/12/2016 Unauthorized Access/Disclosure Email							

Attribution 1 Publication: [hhs.gov](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) Author:
 Article Title: United Community & Family Services
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-03	Florida Department of Health	FL	4/13/2016	Paper Data	Government/Military	Yes - Published #	1,076

More than 1,000 patients of Florida Department of Health clinics in Palm Beach County may be at risk of identity theft after a breach of medical records, state officials disclosed Monday. Federal investigators determined that patient names, Social Security numbers, phone numbers, dates of birth and medical record numbers were among the sensitive information that was taken, according to the Health Department.

Attribution 1 Publication: [hhs.gov / sun-sentinel.com](http://hhs.gov/sun-sentinel.com) Author:
Article Title: Medical records breach affects Palm Beach County patients
Article URL: <http://www.sun-sentinel.com/local/palm-beach/fl-stolen-health-information-palm-20160411-story.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-02	Lake Pulmonary Critical PA	FL	4/20/2016	Paper Data	Medical/Healthcare	Yes - Published #	648

The covered entity (CE), Lake Pulmonary Critical Care, PA, discovered that a former employee removed patient medical records from the office and took them home. The theft of this protected health information (PHI) affected 648 individuals. The medical information included patients' names, addresses, phone numbers, dates of birth, social security numbers, health insurance information, medical diagnoses, lab results, medications, and other treatment information. The CE provided timely breach notification to HHS, to affected individuals, and to the media.

Attribution 1 Publication: hhs.gov Author:
Article Title: Lake Pulmonary Critical PA
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160421-01	Oneida Health Center Dental Clinic	WI	4/21/2016	Electronic	Business	Yes - Published #	2,734

The Oneida Nation is providing this public notification in compliance with federal law. On February 17, 2016 a flash drive containing the limited details of dental patient information was internally stolen from our dental offices at the Oneida Health Center located at 525 Airport Drive, on the Oneida Reservation.

Attribution 1 Publication: [oneidationation.org / hipaajournal.com](http://oneidationation.org/hipaajournal.com) Author:
Article Title: Oneida Health Center Dental Clinic Experiences Data Breach
Article URL: <http://oneidationation.org/newspaper/page.aspx?id=42221>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160420-05	InvenSense, Inc.	CA	4/15/2016	Electronic	Business	Yes - Unknown #	Unknown

InvenSense was the target of an e-mail "phishing" scam. Specifically, on April 12, 2016, an unknown third party sent an email message impersonating our Chief Executive Officer to an InvenSense team member, requesting copies of employee 2015 W -2 tax forms.

Attribution 1 Publication: NH AG's office Author:
Article Title: InvenSense, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/invensense-20160415.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160420-04	Clinton Health Access Initiative	MA	4/5/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

CHAI has determined that a member of its payroll department received a fraudulent email in late March, appearing and purporting to have come from a member of senior leadership within the organization, requesting copies of W-2s of CHAI employees.

Attribution 1 Publication: NH AG's office Author:
Article Title: Clinton Health Access Initiative
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/clinton-health-20160405.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160420-03	Convey Health Solutions	FL	3/21/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On March 7, 2016, we learned that a targeted "spear phishing" email message had been sent to a Convey employee that same day. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. The email our employee received was designed to appear as though it had been sent to the employee by a Convey executive, from the Convey executive's email account, requesting copies of 2015 Forms W-2, including names, addresses, Social Security numbers, and salary information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Convey Health Solutions
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/convey-health-solutions-20160321.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160420-02	Archdiocese of Denver	CO	4/19/2016	Electronic	Business	Yes - Published #	18,000

A third-party software provider that administers the data reported that someone had accessed an archdiocese payroll system and looked at W-2 information for about 80 individuals in October, Keith Parsons, CFO of the archdiocese, said Tuesday.

Attribution 1 Publication: databreaches.net / Denver Post Author: Tom McGhee
Article Title: Denver Archdiocese payroll system breached, 18,000 people at risk
Article URL: http://www.denverpost.com/news/ci_29786064/denver-archdiocese-payroll-system-breached-18-000-at

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160420-01	Pain Treatment Centers of America / Interventional	AR	4/19/2016	Electronic	Medical/Healthcare	Yes - Published #	19,397

Bizmatic. Bizmatic recently informed us that a malicious hacker attacked Bizmatic's data servers, which resulted in unauthorized access to Bizmatic customers' records—ours included. The Prognosis tool stores and organizes patient files, so the information that was potentially compromised is the medical record we maintain on you as a patient, such as health visit information, name, address, health insurance information, driver's license number or other ID and, in some cases, a Social Security number.

Attribution 1 Publication: databreaches.net Author:
Article Title: Pain Treatment Centers of America notifies 19,397 patients of Bizmatic breach
Article URL: <http://www.databreaches.net/pain-treatment-centers-of-america-notifies-19397-patients-of-bizmatic-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160419-03	CVS Alabama Pharmacy	AL	4/19/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

The theft of a laptop computer from an unnamed vendor has exposed the protected health information of a number of Alabama CVS pharmacy patients. The data breach only affects certain patients who have previously filled out prescriptions at a single CVS pharmacy in Alabama. Data stored on the laptop computer included the names of patients along with contact telephone numbers, home addresses, details of the prescriptions provided, and numbers and dispensing dates. No Social Security numbers or financial information were exposed.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Vendor Laptop Theft Exposes PHI of Alabama CVS Pharmacy Patients
Article URL: <http://www.hipaajournal.com/vendor-laptop-theft-exposes-phi-alabama-cvs-pharmacy-patients-3400/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160419-02	Arlington Public Schools	VA	4/19/2016	Electronic	Educational	Yes - Unknown #	Unknown

More than two dozen Arlington Public Schools employees have had their social security numbers and tax information compromised in a data breach, according to a memo sent to APS employees Monday. The breach exposed the W-2 tax forms of 28 APS employees, the school system said. APS issues around 7,000 W-2 forms to employees annually, according to Assistant Superintendent Linda Erdos. The breach occurred on a third-party server and there is no evidence that APS' own systems were compromised, the memo says. However, APS has notified the FBI about the incident.

Attribution 1 Publication: arlnow.com Author:
Article Title: Data Breach Affecting Some APS Employees
Article URL: <https://www.arlnow.com/2016/04/19/data-breach-affecting-some-aps-employees/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160419-01	DoTERRA	UT	4/18/2016	Electronic	Business	Yes - Unknown #	Unknown

We are writing to notify you today that a third-party vendor that provides dōTERRA with data hosting and software services recently informed us that an intruder had accessed some of the vendor's systems.

Attribution 1 Publication: CA AG's office / scmagazine.com / SC A Author:
Article Title: doTERRA
Article URL: https://oag.ca.gov/system/files/doTERRA%20-%20Individual%20Notification%20Letter%20%28California%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-17	Rockhurst University	MO	4/13/2016	Electronic	Educational	Yes - Published #	1,300

The school said about 1,300 people who were employed by Rockhurst in 2015 had their personal information stolen through a targeted phishing scam. Criminals wound up with IRS W-2 forms for those employees.

Attribution 1 Publication: kmbc.com / kansascity.com Author:
Article Title: By KMBC 9 News Staff
Article URL: <http://www.kmbc.com/news/data-breach-affects-hundreds-of-rockhurst-university-employees/39009814>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-16	Office of Virgil Elliot Winn, CPA	SC	3/30/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 27, 2016, YEW learned that a possible security incident may have impacted the security of information stored on its servers. VEW immediately began an investigation and engaged independent, third-party forensic computer experts to assist. While the investigation is still ongoing, it appears that files stored on YEW's system may have been accessed by an unauthorized individual.

Attribution 1 Publication: NH AG's office Author:
Article Title: Office of Virgil Elliot Winn, CPA
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/virgil-winn-20160330.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-15	Silicon Laboratories, Inc.	TX	4/4/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to notify you that on March 30, 2016, Silicon Laboratories, Inc., determined that it had been the victim of an email phishing scheme, which resulted in an unauthorized person or entity obtaining a copy of employee 2015 W-2 forms.

Attribution 1 Publication: NH AG's office Author:
Article Title: Silicon Laboratories, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/silicon-labs-20160404.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-14	Proskauer Rose LLP	NY	4/6/2016	Electronic	Business	Yes - Unknown #	Unknown

After investigating the incident, Proskauer determined that an employee in its payroll department received a fraudulent email requesting copies of W -2s of firm personnel.

Attribution 1 Publication: NH AG's office Author:
Article Title: Proskauer Rose LLP
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/proskauer-rose-20160406.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-13	O'Reilly Media Group	CA	3/31/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 11, 2016, the O'Reilly Media Group discovered that unauthorized access to a database backup file for the O'Reilly School of Technology had occurred. The incident was discovered as the O'Reilly Media Group was shutting down the O'Reilly School of Technology.

Attribution 1 Publication: NH Ag's office / MT AG's office Author:
Article Title: O'Reilly Media Group
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/oreilly-media-20160331.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 172 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-12	OnDeck Capital, Inc.	NY	4/8/2016	Electronic	Business	Yes - Published #	1,570

In November 2015, a company laptop was stolen from an OnDeck employee. Despite an immediate search, the laptop was never recovered. OnDeck has been conducting an investigation of the incident, and has determined that the laptop contained personal information of thirteen (13) New Hampshire residents. The information may have contained names, Social Security numbers and bank account numbers. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: OnDeck Capital, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/ondeck-capital-20160408.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-11	Management Health Systems, Inc. dba MedPro Healthcare	FL	3/15/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On March 8, 2016, we discovered that an employee was the subject of a phishing attack when they received an email purporting to be from the CEO of the company, requesting copies of employee W-2 wage and tax statements. The employee responded to the request and sent electronic copies of the requested documents.

Attribution 1 Publication: Nh AG's office Author:
Article Title: Management Health Systems, Inc. dba MedPro Healthcare Staffing
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/management-health-20160318.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-10	Dixie Group	CA	3/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 9, 2016 we discovered that on February 11, 2016, as a result of a phishing email received by one of our employees, an unauthorized third party received an electronic file containing certain information on all of our current employees, including me.

Attribution 1 Publication: NH AG's office Author:
Article Title: Dixie Group
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/dixie-group-20160321.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-09	Asure Software	TX	4/7/2016	Electronic	Business	Yes - Unknown #	Unknown

On Monday, March 7, 2016, Asure Software was the target of a phishing attack in which hackers posing as an Asure executive successfully requested employee W-2 information via email. Unfortunately, the W-2s were provided before it was discovered that the request was made by what appeared to be the Asure executive's email address.

Attribution 1 Publication: NH AG's office Author:
Article Title: Asure Software
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/asure-software20160407.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-08	Money Now	KY	4/14/2016	Paper Data	Business	Yes - Unknown #	Unknown

Thousands of documents containing personal and financial information were found unshredded and scattered behind the Money Now payday loan business on Taylor Boulevard. Boxes of financial records were found by another business owner in the same strip center who began alerting people he had their information. WAVE 3's Maureen Kyle talked to a woman whose information was discovered, then went to Money Now" for answers.

Attribution 1 Publication: databreaches.net / WAVE3.com Author:
Article Title: Documents Containing Personal Info Found Outside Payday Loan Business
Article URL: <http://www.wave3.com/story/4893150/documents-containing-personal-info-found-outside-payday-loan-business>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-07	Atique Orthodontics	TX	4/18/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

The unauthorized accessing of the computer first occurred on February 29, 2016., with the remote access possible until March 30, 2016., when the security breach was discovered. During the time that remote access was possible, a server containing the protected health information of orthodontics patients could potentially have been accessed

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Atique Orthodontics Reports Potential Breach of Patient PHI
Article URL: <http://www.hipaajournal.com/atique-orthodontics-reports-potential-breach-patient-phi-3398/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-06	Girl Scouts of Gulfcoast Florida, Inc.	FL	3/18/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 17, 2016, we discovered that our company was the targeted victim of an email spoofing attack by an individual or individuals purporting to be me. Through this attack, a request was made for all 2015 employee W2 information. Unfortunately this information was provided before it was discovered that the requests was made from a fraudulent account.

Attribution 1 Publication: VT AG's office Author:
Article Title: Girl Scouts of Gulfcoast Florida, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Girl%20Scouts%20of%20Gulfcoast%20Florida_%20Inc

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-05	Town of Essex	VT	4/13/2016	Electronic	Government/Military	Yes - Published #	262

On April 7th & 8th, 2016 an unknown person sent fraudulent emails to the Town of Essex staff, pretending to be a Town Official. This email requested payroll records for all Town personnel. Mistakenly, town staff did not confirm the identity of the sender and sent the requested payroll records in response to the fraudulent emails.

Attribution 1 Publication: VT AG's office Author:
Article Title: Town of Essex
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Town%20of%20Essex%20SBN%20to%20Consumers.p

Attribution 2 Publication: vtdigger.com Author:
Article Title: Town of Essex
Article URL: <http://vtdigger.org/2016/04/19/178902/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-04	Examination Management Services, Inc. (EMSI)	TX	4/6/2016	Electronic	Business	Yes - Published #	4,965

On March 24, 2016, in what is known as a "spoofing" attack, an unknown third party sent us an email from what appeared to be an authorized internal company account requesting employee W-2 forms. Copies of 2015 W-2 forms were sent in response to this email

Attribution 1 Publication: VT AG's office / NH AG's office / IN AG's Author:
Article Title: Examination Management Services, Inc. (EMSI)
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/EMSI%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-03	Academy of Art University	NC	4/13/2016	Electronic	Educational	Yes - Unknown #	Unknown

On March 4, 2016, an employee of the Academy was targeted by an e-mail scam, called "spoofing." The spoofed e-mail appeared to come from a member of the Academy's executive team and asked for employees' W-2 information. Because the recipient/employee wrongly believed the e-mail to contain a valid request from a senior executive, the employee replied by attaching the federal Form W-2 for you and other Academy employees.

Attribution 1 Publication: CA AG's office / NH AG's office / MT AG' Author:
Article Title: Academy of Art University
Article URL: https://oag.ca.gov/system/files/Academy%20of%20Art%20Notice%20Letter%20%28002%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-02	Olympia School District	WA	4/13/2016	Electronic	Educational	Yes - Published #	2,164

An email -- configured in a way to look as though it had originated from Olympia Superintendent Dick Cvitanich's school district account -- was sent to an employee requesting a list of employee names, addresses, salary information and Social Security numbers, officials say.

Attribution 1 Publication: securityinfowatch.com / WA AG's office Author: Lisa Pemberton
Article Title: Wash. school district suffers data breach
Article URL: <http://www.securityinfowatch.com/news/12195164/wash-school-district-suffers-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160418-01	WLNE-TV	RI	4/17/2016	Electronic	Business	Yes - Unknown #	Unknown

The letter, signed by vice president and general manager Christopher S. Tzianabos, said that on April 8 it was discovered a computer file containing personnel information had been placed on the station's shared drive and accessed by various employees. The file included names, Social Security numbers, driver's license numbers, bank account and credit card numbers, employment contracts, evaluations, and separation agreements. The file has since been removed.

Attribution 1 Publication: WN.com Author:
Article Title: Data breach at TV station reveals personnel information
Article URL: http://article.wn.com/view/2016/04/17/Data_breach_at_TV_station_reveals_personnel_information/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160415-02	American College of Cardiology (ACC)	DC	4/14/2016	Electronic	Business	Yes - Unknown #	Unknown

The American College of Cardiology (ACC) notified 1,400 institutions that patient data from the National Cardiovascular Data Registry (NCDR) might have been breached. After discovering the issue in December, the ACC found that four software development vendors who were testing software had access to NCDR patient data, according to the ACC.

Attribution 1 Publication: cardiovascularbusiness.com Author: Tim Casey
Article Title: ACC notifies 1,400 institutions of potential data breach
Article URL: <http://www.cardiovascularbusiness.com/topics/practice-management/acc-notifies-1400-institutions-potential-data-bre>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160415-01	City of Baltimore	MD	4/15/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

The data breach was discovered when several city employees attempted to electronically file tax returns, which were rejected because their returns had already been filed. The city is working with local, state and federal authorities to try to figure out how this could have happened. It remains unclear from which entity the data was taken.

Attribution 1 Publication: WBALtv.com Author:
Article Title: Baltimore City employees' information stolen
Article URL: <http://www.wbal.com/news/data-breach-hits-baltimore-city-workers-official-confirms/39037196>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160412-04	Schwaab, Inc. (Discount Rubber Stamps.com)	WI	2/4/2016	Electronic	Business	Yes - Published #	85,000

We recently learned that sometime between January 22, 2014 and January 26, 2016, our computer system was accessed without our authorization. During this time, it is possible that our customer credit card information may have been compromised. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: Schwaab, Inc.
Article URL: https://oag.ca.gov/system/files/Schwaab%20Notification%20Letter_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160412-03	Staminus Communications	CA	4/11/2016	Electronic	Business	Yes - Published #	3,338

On March 10, 2016, Staminus Communications was the victim of an unauthorized intrusion into its network. As a result of this intrusion, systems were temporarily taken offline and customer information was exposed. The protection of the personal information of its customers is very important to Staminus. Based on our initial investigation, we know that names and credit card numbers, as well as usernames, passwords, and contact information, were exposed. Staminus' investigation into the incident is ongoing. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
 Article Title: Staminus Communications
 Article URL: <https://oag.ca.gov/system/files/Sample%20Customer%20Notice%20-%20CC%2C%20Username%2C%20and%20Passw>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160412-02	Bristol Farms	CA	4/8/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 30, 2016, an unauthorized individual, impersonating a Bristol Farms/Lazy Acres executive, contacted Bristol Farms/Lazy Acres requesting certain information for Bristol Farms/Lazy Acres employees. Before it was determined that the request was fraudulent, an electronic file was provided, which contained information about the affected employees.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Bristol Farms
 Article URL: https://oag.ca.gov/system/files/Sample%20Notice_6.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160412-01	Stanford University / Equifax W-2Express	CA	4/12/2016	Electronic	Educational	Yes - Published #	600

At least 600 current and former Stanford employees are vulnerable to tax fraud following the illegitimate download of their W-2 forms through a third-party service.

Attribution 1 Publication: stanforddaily.com / VT AG's office / MD Author:
 Article Title: University employees vulnerable after tax data breach
 Article URL: <http://www.stanforddaily.com/2016/04/12/university-employees-vulnerable-after-tax-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160411-05	Federal Deposit Insurance Corp. (FDIC)	DC	4/11/2016	Electronic	Government/Military	Yes - Published #	44,000

The former employee, who was not identified, left FDIC on February 26 with the personal storage device. Using technology to track downloads to removable devices, FDIC detected the breach on February 29 and the employee returned it the next day. "The FDIC's relationship with the employee has not been adversarial," the memo said.

Attribution 1 Publication: Federal Times Author: Aaron Boyd
 Article Title: FDIC waited months to report major October data breach
 Article URL: <http://www.federaltimes.com/story/government/cybersecurity/2016/04/20/fdic-major-breach/83233956/>

Attribution 2 Publication: washingtonpost.com / databreaches.net Author:
 Article Title: 'Inadvertent' cyber breach hits 44,000 FDIC customers
 Article URL: <https://www.washingtonpost.com/news/powerpost/wp/2016/04/11/inadvertent-cyber-breach-hits-44000-fdic-customers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160411-04	Department of Health - Palm Beach County	FL	4/11/2016	Electronic	Government/Military	Yes - Published #	1,000

Florida Department of Health in Palm Beach County is issuing a public notice of an unauthorized disclosure and/or use of protected health information pertaining to some clients of its Health Centers. Federal law enforcement officials informed the department they had obtained a list of names, birth dates, social security numbers, Medicaid numbers, phone numbers, and medical record numbers of individuals who were identified as Palm Beach County Health Department clien

Attribution 1 Publication: databreaches.net Author:
Article Title: FL Dept. of Health Palm Beach County Notification of Breach
Article URL: <http://www.databreaches.net/fl-dept-of-health-palm-beach-county-notification-of-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160411-03	Randolph College	VA	4/11/2016	Electronic	Educational	Yes - Published #	100

The situation is being investigated by Lynchburg Police and the FBI, but Edson says the problem did not originate on campus. She and campus administrators believe one possible culprit could be the online program Randolph uses to distribute tax forms to its employees.

Attribution 1 Publication: databreaches.net / WDBJ7.com Author:
Article Title: More than 100 Randolph College employees report recent identity theft
Article URL: <http://www.wdbj7.com/news/local/more-than-100-randolph-college-employees-report-identity-theft/38973582>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160411-02	Office of Child Support Enforcement	WA	4/6/2016	Electronic	Government/Military	Yes - Published #	5,000,000

Nearly five million people may have had their sensitive information compromised after a personal laptop was taken from a federal building in Washington state in February, but the breach wasn't reported until late March, prompting Congress members to question the breach response actions taken by HHS, reports The Associated Press. Burglars reportedly broke into the Office of Child Support Enforcement in Olympia, Wash., and stole hard drives and a personal laptop. The hard drives may have contained up to 5 million names and Social Security numbers, according to the report.

Attribution 1 Publication: Beckershospitalreview.com Author:
Article Title: HHS under fire for delayed data breach report
Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/hhs-under-fire-for-delayed-data-breach-rep>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160411-01	OptumRx	MN	3/16/2016	Electronic	Medical/Healthcare	Yes - Published #	6,229

We wanted to make you aware of a recent incident that may have affected some of your health information. On March 22, 2016, we were notified that an unencrypted laptop computer belonging to a vendor of OptumRx, which provides home delivery prescription services to you, was stolen from one of its employee's vehicles. The theft occurred on March 16, 2016 in Indianapolis, Indiana.

Attribution 1 Publication: CA AG's office Author:
Article Title: OptumRx
Article URL: <https://oag.ca.gov/system/files/individual%20notification%20letter%20optumrx%20vendor%20laptop%20matter%20-%>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160408-03	Einstein Health Network	PA	4/7/2016	Electronic	Medical/Healthcare	Yes - Published #	2,939

On February 2, 2016, we learned that a website database containing information entered into our website "Request for Information" form, which contained patient information, had inadvertently been left accessible via the internet.

Attribution 1 Publication: databreaches.net / EHN notice Author:
Article Title: Einstein Health Network notifies 3,000 patients after web exposure of information
Article URL: <http://www.databreaches.net/einstein-health-network-notifies-3000-patients-after-web-exposure-of-information/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160408-02	Wallys Wine and Spirits	CA	4/8/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that we, too, have been victimized by such an intrusion. While reviewing security logs on or about December 30, 2015, our IT Manager noticed unusual activity. We promptly began an investigation, which has now determined that several unauthorized user accounts were used to gain access to our system and view certain information, as set forth below.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Wallys Wine and Spirits
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Wallys%20Wine%20and%20Spirits%20SBN%20to%20C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160408-01	Whiting Turner Contracting Company	MD	3/8/2016	Electronic	Business	Yes - Published #	5,904

Was Involved? If your child is a minor dependent who received healthcare insurance coverage under a policy for which the primary policyholder was a current, former, or retired employee, we believe this incident may affect the security of your child's information contained on that employee policyholder's 2015 IRS Form 1095, which includes the following: name, date of birth, and Social Security number of any minor dependent. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
 Article Title: Whiting Turner Contracting
 Article URL: <https://oag.ca.gov/system/files/Whiting%20Turner%20Contracting%20NOTICE%20only%20CA%20Regulator%20Notice>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160406-07	Norfolk Admirals	VA	3/30/2016	Electronic	Business	Yes - Unknown #	Unknown

The Norfolk Admirals Vice President Joe Gregory tells WAVY.com a hacker got into the Admirals system and obtained email addresses, names and home addresses. The breach did not include sensitive credit card or bank account information.

Attribution 1 Publication: WAVY.com Author:
 Article Title: Norfolk Admirals confirm data breach exposing customers' information
 Article URL: <http://wavy.com/2016/03/30/norfolk-admirals-confirm-data-breach-exposing-customers-information/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160406-06	Escambia County School System	FL	4/6/2016	Electronic	Educational	Yes - Unknown #	Unknown

The Escambia County School System is one of three in the state hit with a payroll accounting system security breach that allowed fraudulent tax returns to be filed in employee names.

Attribution 1 Publication: databreaches.net / brewtonstandard.co Author:
 Article Title: Escambia County School hit with payroll system security breach
 Article URL: <http://www.brewtonstandard.com/2016/04/06/escambia-county-school-hit-with-payroll-system-security-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160406-05	Lindsay House Surgery Center	NY	3/18/2016	Electronic	Medical/Healthcare	Yes - Published #	773

Hospital for Special Surgery NY Healthcare Provider 647 3/17/2016 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: Lindsay House Surgery Center
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160406-04	Excel Plus Home Health, Inc.	TX	3/23/2016	Electronic	Medical/Healthcare	Yes - Published #	524

Excel Plus Home Health, Incorporated TX Healthcare Provider 524 03/23/2016 Theft Desktop Computer

Attribution 1 Publication: hhs.gov Author:
 Article Title: Excel Plus Home Health, Inc.
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 178 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160406-03	NRT	NJ	3/22/2016	Electronic	Business	Yes - Unknown #	Unknown

Based on our investigation, affected residents' personal information may have been included in the body of an email or attachment within an affected agent's account. The types of personal information exposed vary depending on what was sent by email but may include affected residents' Social Security numbers, passport numbers, driver's license or state identification numbers, or credit card numbers. We have no evidence that any personal information was used to commit identity theft.

Attribution 1 Publication: NH AG's office Author:
Article Title: NRT
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/nrt-20160322.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160406-02	Universal Service Administrative Company	DC	3/31/2016	Electronic	Business	Yes - Published #	Unknown

On March 24, 2016, a USAC employee was the victim of a sophisticated "phishing" email that appeared to be from the employee's superior and requested the 2015 IRS W-2 forms of USAC employees. The employee provided the 2015 W-2 information because the email address had been masked to appear as if the email came from the actual superior's USAC email address.

Attribution 1 Publication: VT AG's office Author:
Article Title: Universal Service Administrative Company (USAC)
Article URL: http://www.ago.vermont.gov/assets/files/Consumer/Security_Breach/2016-04-05%20Universal%20Service%20Administ

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160406-01	Katherman Kitts & Co.	CA	4/5/2016	Electronic	Business	Yes - Published #	1,407

On February 25, 2016, hard drives containing backup files for one of the firm's servers, along with other incidental items, were stolen from a partner's locked vehicle. These files may have contained some of your confidential information as a client of Katherman Kitts & Co. LLP. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: Katherman Kitts & Co.
Article URL: https://oag.ca.gov/system/files/Katherman.CA_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-14	Kentucky State University	KY	3/31/2016	Electronic	Educational	Yes - Published #	1,071

Kentucky State University was hit with a data breach on March 22 when an employee, responding to an email supposedly from the school's president, sent off W-2s for employees and students. 2015 W-2s and university identities for employees and students, including names, Social Security numbers and addresses.

Attribution 1 Publication: scmagazine.com Author: Greg Masters
Article Title: Data on 1K staffers and students at Kentucky State University exposed
Article URL: <http://www.scmagazine.com/data-on-1k-staffers-and-students-at-kentucky-state-university-exposed/article/486507/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-13	Indian Health Service / Norther Navajo Medical	NM	4/5/2016	Paper Data	Medical/Healthcare	Yes - Published #	7,421

The medical records of approximately 7,500 patients of an Indian Health Service medical center have been recovered from storage units in Waterflow in New Mexico, at least 5 months after they were stolen by a former employee.

Back in October, the records of 470 patients of the Northern Navajo Medical Center in Shiprock were found in a public storage facility by a community member. The matter was reported to the Navajo Area Indian Health Service on October 5, 2015, and staff were sent to recover the documents.

According to the IHS breach notice, the Department of Health and Human Services Office of Inspector General Investigator investigated the breach and discovered that files had been taken by a former employee. Some of the employee's personal items were also located in the storage facility.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 7,500 Patients Notified of Indian Health Service PHI Theft
Article URL: <http://www.hipaajournal.com/7500-patients-notified-of-indian-health-service-phi-theft-3384/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-12	Kings Daughters Health	IN	4/5/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Kings Daughters Health (KDH), an Indiana hospital, also reported that it had suffered a recent ransomware attack. KDH shut down all computer systems last Wednesday when it realized that a single user's files were infected with the ransomware, according to Indiana radio station Eagle Country 99.3.

Attribution 1 Publication: healthitsecurity.com / databreaches.net Author:
Article Title: King's Daughters' Health shut down systems after Locky detected.
Article URL: <http://www.databreaches.net/kings-daughters-health-shut-down-systems-after-locky-detected/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-11	Alvarado Hospital Medical Center / Prime Healthcare	CA	4/5/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

San Diego, California-based Alvarado Hospital Medical Center reportedly had a "malware disruption" earlier this week. The computer systems were recovered without having to pay a ransom, according to the San Diego Union-Tribune.

Attribution 1 Publication: healthitsecurity.com Author: Elizabeth Snell
Article Title: More Hospitals Affected by Healthcare Ransomware Attacks
Article URL: <http://healthitsecurity.com/news/more-hospitals-affected-by-healthcare-ransomware-attacks>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-10	Mohawk Mountain Ski Area	CT	3/28/2016	Electronic	Business	Yes - Unknown #	Unknown

During the week of March 15, 2016, we learned that direct deposit information for some our employees had been changed. We immediately began an investigation, contacted our payroll vendor, changed the direct deposit information so that no unauthorized transfers occurred, and changed the credentials to our payroll provider's portal. We confirmed that an unauthorized individual had gained access to our payroll vendor's portal and had changed your direct deposit information. In addition to your bank account and routing numbers, the unauthorized individual had the ability to access your personal information in our payroll provider portal, such as your name, address, telephone number, date of birth, wages, employee identification number, and Social Security number.

Attribution 1 Publication: VT AG's office Author:
Article Title: Mohawk Mountain Ski Area
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Mohawk%20Mountain%20Ski%20Area_%20Inc.%20SB

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-09	Traphagen & Traphagen CPAs	NJ	3/29/2016	Electronic	Business	Yes - Unknown #	Unknown

We noticed several client IRS tax filings were not accepted and also several clients received letters from the IRS. We notified our external IT expert and began to investigate this activity that occurred between September 14, 2015 and September 24, 2015. Our IT expert identified unauthorized access of data in our document retention system. We discovered this on February 24, 2016.

Attribution 1 Publication: VT AG's office Author:
Article Title: Traphagen & Traphagen CPAs
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Traphagen%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-08	Champlain Oil	VT	3/30/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 15, 2016 an unidentified third party obtained access to Champlain employees' W -2 information for calendar year 2015 through an email phishing scheme. The W-2's contained employee names, addresses, Social Security numbers and 2015 wages earned. The unauthorized third party also obtained costs of company-paid benefits for health insurance, contributions to retirement, and taxes withheld from employee earnings.

Attribution 1 Publication: Author:
 Article Title: Champlain Oil
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Champlain%20Oil%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-07	IASIS Healthcare	TN	4/4/2016	Electronic	Medical/Healthcare	Yes - Published #	18,273

The week of March 21, 2016, an unauthorized individual, impersonating an IASIS executive, contacted an IASIS employee requesting certain information for IASIS employees. Before it was determined that the request was fraudulent, the IASIS employee provided a file that contained limited information about some of our employees. The files contained employee information including first and last name, Social Security number, and 2015 compensation and deduction information. Employee's home addresses and dates of birth were not provided. Note that our information technology system was not compromised and no protected health information about any employee or patient was provided to any unauthorized individual. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / IN AG's office / MD AG' Author:
 Article Title: IASIS Healthcare
 Article URL: http://www.ago.vermont.gov/assets/files/Consumer/Security_Breach/2016-04-04%20IASIS%20Healthcare%20SBN%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-06	ARC International North America, LLC	NJ	3/28/2016	Electronic	Business	Yes - Unknown #	Unknown

On Friday, March 11, 2016, certain personal information of current and former employees of ARC International North America, LLC, Cardinal International III, LLC and Durand Glass Manufacturing Company, LLC (collectively "ARC") was mistakenly transmitted by ARC via email to a third party posing as an officer of ARC. Those W-2 form copies included the name, address, city, state, zip code, Social Security number, gross compensation amount, federal income tax withholding amount, Social Security wage and tax withholding amounts, Medicare wage and tax withholding amounts, gross state compensation amount, and state income tax withholding amount (and comparable local tax information) of each such person.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
 Article Title: ARC International North America, LLC
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/ARC%20International%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-05	Morton Medical Center PLLC	WA	3/24/2016	Electronic	Medical/Healthcare	Yes - Published #	3,000

Morton Medical Center, PLLC WA Healthcare Provider 3000 03/24/2016 Hacking/IT Incident Desktop Computer, Network Server

Attribution 1 Publication: hhs.gov Author:
 Article Title: Morton Medical Center PLLC
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-04	Aurora Health Care, Inc.	WI	4/1/2016	Electronic	Medical/Healthcare	Yes - Published #	869

Aurora Health Care, Inc. WI Healthcare Provider 869 04/01/2016 Unauthorized Access/Disclosure Network Server

Attribution 1 Publication: hhs.gov Author:
 Article Title: Aurora Health Care, Inc.
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-03	Pointe Medical Services, Inc.	FL	4/1/2016	Electronic	Medical/Healthcare	Yes - Published #	2,000

A former employee of Pointe Medical Services has been accused of stealing the protected health information of patients and disclosing the data to her new employer, with a view to soliciting patients and encouraging them to change healthcare providers.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](http://hhs.gov/hipaajournal.com) Author:
Article Title: ROGUE EMPLOYEE STEALS PHI OF 2,000 POINTE MEDICAL SERVICES PATIENTS
Article URL: <http://www.hipaajournal.com/rogue-employee-steals-phi-of-2000-pointe-medical-services-patients-3385/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-02	Metropolitan Jewish Health System, Inc.	NY	3/22/2016	Electronic	Medical/Healthcare	Yes - Published #	2,483

Metropolitan Jewish Health System, Inc., (MJHS) is the latest healthcare organization to announce it has fallen victim to a phishing attack. The incident appears to have resulted in one email account being compromised, although an investigation is still ongoing to determine if any other email accounts were also affected.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](http://hhs.gov/hipaajournal.com) / MT AG's off Author:
Article Title: Metropolitan Jewish Health System, Inc.
Article URL: <http://www.hipaajournal.com/phishing-attack-reported-by-metropolitan-jewish-health-system-inc-3383/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160405-01	Information Resources, Inc.	IL	3/23/2016	Electronic	Business	Yes - Published #	1,297

On March 10, 2016, a company laptop was stolen from an IRI employee. The theft was reported to law enforcement authorities. At this time, it appears that the theft was a random criminal act, and we have no reason to believe that any of the information on the laptop has been accessed or misused. The stolen laptop requires a password to access information stored on it. Files on the laptop may have contained your name, Social Security number, and other personal information. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / IN AG's office Author:
Article Title: Information Resources, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Information%20Resources%20Inc%20SBN%20to%20C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160404-09	Val Verde Regional Medical Center	TX	3/18/2016	Electronic	Medical/Healthcare	Yes - Published #	2,000

On or about Aug. 9, 2015, an independent healthcare provider downloaded unsecured protected health information and emailed it to a personal account without encryption protection. In addition, the independent contractor was not authorized to access some of the protect health information.

Attribution 1 Publication: delrionewsherald.com Author:
Article Title: Russells True Value 728x90
Article URL: http://delrionewsherald.com/news/article_2525f1ca-f75b-11e5-acfe-875b966d8a87.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160404-08	Cardiology Associates of Jonesboro, Inc.	AR	3/4/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,669

Cardiology Associates of Jonesboro, Inc. AR Healthcare Provider 1669 03/04/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Cardiology Associates of Jonesboro, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160404-07	Group Life Hospital and Medical Program	CT	2/29/2016	Electronic	Medical/Healthcare	Yes - Published #	3,000

Group Life Hospital and Medical Program CT Health Plan 3000 02/29/2016 Hacking/IT Incident Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Group Life Hospital and Medical Program
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 182 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160404-06	Ecolab Health and Welfare Benefits Plan	MN	2/26/2016	Electronic	Medical/Healthcare	Yes - Published #	1,550
Ecolab Health and Welfare Benefits Plan MN Health Plan 1550 02/26/2016 Hacking/IT Incident Network Server							

Attribution 1 Publication: hhs.gov Author:
Article Title: Ecolab Health and Welfare Benefits Plan
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160404-05	Bozeman Health Deaconess Hospital	MT	3/21/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,124
Bozeman Health Deaconess Hospital MT Healthcare Provider 1124 03/21/2016 Unauthorized Access/Disclosure Paper/Films							

Attribution 1 Publication: hhs.gov Author:
Article Title: Bozeman Health Deaconess Hospital
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160404-04	Wells Fargo ATMs	CA	4/3/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

In San Diego County, investigators say the latest major breach is the work of one man, seen on ATM surveillance cameras during the first few months of this year wearing the same ball cap. Atef Alkhateeb, 42, is accused of placing skimming devices on Wells Fargo ATMs throughout the county that stole personal information from debit and credit cards. Armed with that sensitive data, federal investigators say Alkhateeb then created counterfeit cards and looted nearly a half-million dollars total from bank accounts — sending a significant amount of that money to Jordan and other foreign countries.

Attribution 1 Publication: sandiegouniontribune.com Author:
Article Title: Thousands of cards compromised in ATM scam
Article URL: <http://www.sandiegouniontribune.com/news/2016/apr/03/atm-skimming-arrest-alkhateeb/all/?print>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160404-03	MedStar Health	DC	3/28/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

In MedStar's case, a virus early this week infiltrated its computer systems, forcing the health-care giant to shut down its entire network, turn away patients, postpone surgeries and resort to paper records.

Attribution 1 Publication: Tyler Morning Telegraph / MD AG's offic Author:
Article Title: Hospitals are hackers' biggest new target with digital records of patient data
Article URL: <http://www.tylerpaper.com/TP-News+National/233665/hospitals-are-hackers-biggest-new-target-with-digital-records-of->

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160404-02	Blue Chip Dental	MI	3/29/2016	Electronic	Medical/Healthcare	Yes - Published #	2,200

2,200 Blue Chip Dental patients have been notified that a backup system installed to safeguard patients' protected health information (PHI) has played a part in its exposure. The Social Security numbers, medical insurance information, names, and addresses of patients have potentially been compromised as a result of the loss of a portable storage device used to store data backups.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 2,200 MICHIGAN DENTAL PATIENTS NOTIFIED OF PHI BREACH
Article URL: <http://www.hipaajournal.com/2200-michigan-dental-patients-warned-of-phi-breach-3374/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 183 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160404-01	Trump Hotels	NY	4/4/2016	Electronic	Business	Yes - Unknown #	Unknown

Banking industry sources tell KrebsOnSecurity that the Trump Hotel Collection — a string of luxury properties tied to business magnate and Republican presidential candidate Donald Trump — appears to be dealing with another breach of its credit card systems. If confirmed, this would be the second such breach at the Trump properties in less than a year.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Trump Hotels Breached Again
Article URL: <http://krebsonsecurity.com/2016/04/sources-trump-hotels-breached-again/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160401-02	Pivotal Software, Inc.	CA	3/22/2016	Electronic	Business	Yes - Unknown #	Unknown

Pivotal was recently involved in an e-mail “phishing” scam targeting personal information of Pivotal employees. On March 22, 2016, an unknown third party sent a fraudulent email message impersonating CEO Rob Mee to an employee requesting certain information about Pivotal employees. The employee responded to the request, mistakenly believing that it came from .Mr. Mee.

Attribution 1 Publication: CA AG's office Author:
Article Title: Pivotal Software, Inc.
Article URL: https://oag.ca.gov/system/files/Sample%20of%20Notice%20to%20California%20residents_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160401-01	Ullrich Delevati	CA	3/28/2016	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that a number of our clients had 2015 tax returns filed in their names without their authorization. We immediately engaged a digital forensics firm to help us investigate whether our information system had been accessed without authorization. On March 15, 2016 we received confirmation from the digital forensics firm that some client information may have been accessed without our authorization.

Attribution 1 Publication: CA AG's office / MT AG's office Author:
Article Title: Ullrich Delevati
Article URL: https://oag.ca.gov/system/files/Ullrich%20Delevati%20notification%20letter_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160329-07	Northgate Medical	MA	3/28/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Northgate said they discovered in January that a former employee had taken a list of patients and left the practice. The list included patient names, addresses, phone numbers, ages, and dates of birth. It did not include social security, account numbers, or medical information relating to patients.

Attribution 1 Publication: databreaches.net / WWLP.com Author:
Article Title: Patient information taken from Northgate Medical
Article URL: <http://wwlp.com/2016/03/28/patient-information-taken-from-northgate-medical/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160329-06	Community in Action	GA	3/29/2016	Paper Data	Business	Yes - Unknown #	Unknown

The director of the non-profit organization, Community in Action, left town and abandoned donations along with her clients' personal information. Her landlord discovered copies clients' social security cards, drivers' licenses and birth certificates left in the home. Ward's former landlord also discovered something else left behind. "People's social security numbers that were supposed to be recipients includes birth certificates all their vital information," she said. We counted thirty-four files full of personal documents from people who applied for assistance with Community in Action. "I knew something was wrong here," Wilcher said.

Attribution 1 Publication: wrdw.com Author:
Article Title: Community in Action
Article URL: <http://www.wrdw.com/home/headlines/OYS-Non-profit-director-leaves-town--373768631.html>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 184 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160329-05	Ryman Hospitality Properties	TN	3/29/2016	Electronic	Business	Yes - Published #	2,478

Nashville's Ryman Hospitality Properties has fallen victim to a fraudulent phishing scam that resulted in employees' IRS W-2 information, which includes Social Security numbers, being disclosed externally, Billboard has learned. (Consumers affected per IN AG's office)

Attribution 1 Publication: billboard.com / IN AG's office Author:
Article Title: Grand Ole Opry Parent Company Falls Victim to Phishing Scam
Article URL: <http://www.billboard.com/articles/business/7311626/ryman-properties-grand-ole-opry-parent-company-victim-irs-phish>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160329-04	Mind Springs Health	CO	2/27/2016	Electronic	Medical/Healthcare	Yes - Published #	2,147

Mind Springs Health, a Colorado-based provider of mental health and substance abuse services, appears to also have been affected. 2,147 patients have now been notified that their PHI has been exposed as a result of a server misconfiguration error made by an unnamed transcription service provider.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: VENDOR ERROR PLACES MIND SPRINGS HEALTH PATIENTS' PHI IN SEARCH ENGINES
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160329-03	Walgreen Co.	IL	3/4/2016	Electronic	Medical/Healthcare	Yes - Published #	880

Walgreen Co. IL Healthcare Provider 880 03/04/2016 TheftPaper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Walgreen Co.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160329-02	Office of W. Christopher Bryant DDS	MI	3/17/2016	Electronic	Medical/Healthcare	Yes - Published #	2,200

You are receiving this letter because of a recent incident that may have exposed your name, address, social security number and insurance information to outside agents. To give you some background information on what happened, on January 26th (2016) we were unable to locate a portable backup hard drive used to store our digital information offsite in case of fire or other disaster to our building.

Attribution 1 Publication: hhs.com / databreaches.net Author:
Article Title: Michigan Dentist notifies patients of missing backup drive
Article URL:

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160329-01	Hospital for Special Surgery	NY	3/17/2016	Electronic	Medical/Healthcare	Yes - Published #	647

Hospital for Special Surgery NY Healthcare Provider 647 03/17/2016 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Hospital for Special Surgery
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160328-02	Mercy Iowa City / Mercy Clinics	IN	3/25/2016	Electronic	Medical/Healthcare	Yes - Published #	15,625

Patients started to be notified of the security breach by mail on Friday March 25, 2016., and have been informed that their name, address, date of birth, medical diagnoses, treatment information, and health insurance details – including their policy number and provider name – may have been compromised. Some Social Security numbers could also have been improperly accessed as a result of the infection.

Attribution 1 Publication: kcci.com / hipaajournal.com Author:
Article Title: DATA-CAPTURING VIRUS DISCOVERED BY MERCY HOSPITAL IN IOWA CITY
Article URL: <http://www.hipaajournal.com/data-capturing-virus-discovered-by-mercy-hospital-in-iowa-city-3373/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160328-01	Aspiranet	CA	3/28/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 21, 2016, Aspiranet was targeted by an e-mail scam called "spoofing." We discovered this incident within thirty minutes of it taking place. Nonetheless, it resulted in Aspiranet inadvertently making personal information from your W-2 filing available to a third party.

Attribution 1 Publication: CA AG's office Author:
Article Title: Aspiranet
Article URL: https://oag.ca.gov/system/files/W2%20Incident%20-%20notice%20attachment_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160325-01	Tidewater Community College	VA	3/25/2016	Electronic	Educational	Yes - Published #	3,193

According to school officials, it was learned a day ago that a file containing the names of all 2015 TCC employees, their social security numbers, 2015 earnings, withholding and deduction information was sent in response to a request that looked to be from a legitimate TCC account.

Attribution 1 Publication: WAVY.com Author:
Article Title: Tidewater Community College announces major data breach
Article URL: <http://wavy.com/2016/03/25/tidewater-community-college-announces-serious-data-breach/>

Attribution 2 Publication: ABC13NewsNow.com / MD AG's letter Author:
Article Title: Employee data breach reported at TCC
Article URL: <http://www.13newsnow.com/news/employee-data-breach-reported-at-tcc/102256781>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-13	Netcracker Technology Corporation	MA	3/17/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 10, 2016, a Netcracker employee received an e-mail that identified Netcracker's Chief Executive Officer as the purported sender. That e-mail requested employees' W-2 information. Because the employee wrongly believed the e-mail was a valid request, the employee replied by attaching employees' federal Form W-2s.

Attribution 1 Publication: NH AG's office Author:
Article Title: Netcracker Technology Corporation
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/netcracker-20160317.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-12	Medieval Times	CA	3/24/2016	Electronic	Business	Yes - Unknown #	Unknown

Over the past week, KrebsOnSecurity similarly has heard from employees at a broad range of organizations that appear to have fallen victim to W2 phishing scams, including the jousting-and-feasting entertainment company Medieval Times.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Medieval Times
Article URL: <http://krebsonsecurity.com/2016/03/phishing-victims-muddle-tax-fraud-fight/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-11	QTI Group	WI	3/24/2016	Electronic	Business	Yes - Unknown #	Unknown

Over the past week, KrebsOnSecurity similarly has heard from employees at a broad range of organizations that appear to have fallen victim to W2 phishing scams, including: QTI Group, a Wisconsin-based human resources consulting company.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: QTI Group
Article URL: <http://krebsonsecurity.com/2016/03/phishing-victims-muddle-tax-fraud-fight/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-10	Nation's Lending Corporation	OH	3/24/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Over the past week, KrebsOnSecurity similarly has heard from employees at a broad range of organizations that appear to have fallen victim to W2 phishing scams, including: Nation's Lending Corporation, a mortgage lending firm in Independent, Ohio.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Nation's Lending Corporation
Article URL: <http://krebsonsecurity.com/2016/03/phishing-victims-muddle-tax-fraud-fight/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-09	Century Fence	WI	3/24/2016	Electronic	Business	Yes - Unknown #	Unknown

Over the past week, KrebsOnSecurity similarly has heard from employees at a broad range of organizations that appear to have fallen victim to W2 phishing scams, including: Century Fence, a fencing company in Wisconsin.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Century Fence
Article URL: <http://krebsonsecurity.com/2016/03/phishing-victims-muddle-tax-fraud-fight/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-08	Aspect	AZ	3/24/2016	Electronic	Business	Yes - Published #	1,300

Over the past week, KrebsOnSecurity similarly has heard from employees at a broad range of organizations that appear to have fallen victim to W2 phishing scams, including call center software provider Aspect. (Consumers affected per IN AG's office)

Attribution 1 Publication: krebsonsecurity.com / IN AG's office Author:
Article Title: Aspect
Article URL: <http://krebsonsecurity.com/2016/03/phishing-victims-muddle-tax-fraud-fight/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-07	Kantar Group (TNS)	NY	3/24/2016	Electronic	Business	Yes - Published #	28,000

Over the past week, KrebsOnSecurity similarly has heard from employees at a broad range of organizations that appear to have fallen victim to W2 phishing scams, including some 28,000 employees of the market research giant Kantar Group.

Attribution 1 Publication: krebsonsecurity.com / MD AG's office Author:
Article Title: Kantar Group (TNS)
Article URL: <http://krebsonsecurity.com/2016/03/phishing-victims-muddle-tax-fraud-fight/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-06	ISCO Industries, Inc.	KY	3/7/2016	Electronic	Business	Yes - Published #	180

W2 phishers hauled in tax data on an estimated 180 employees of ISCO Industries in Huntsville

Attribution 1 Publication: krebsonsecurity.com / ME AG's office / Author:
Article Title: ISCO Industries, Inc.
Article URL: <http://krebsonsecurity.com/2016/03/phishing-victims-muddle-tax-fraud-fight/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 187 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-05	Verizon Enterprise Solutions	NJ	3/24/2016	Electronic	Business	Yes - Published #	1,500,000

Verizon Enterprise Solutions, a B2B unit of the telecommunications giant that gets called in to help Fortune 500's respond to some of the world's largest data breaches, is reeling from its own data breach involving the theft and resale of customer data, KrebsOnSecurity has learned. Earlier this week, a prominent member of a closely guarded underground cybercrime forum posted a new thread advertising the sale of a database containing the contact information on some 1.5 million customers of Verizon Enterprise.

Attribution 1 Publication: [krebsonsecurity.com](#) Author:
Article Title: Crooks Steal, Sell Verizon Enterprise Customer Data
Article URL: <http://krebsonsecurity.com/2016/03/crooks-steal-sell-verizon-enterprise-customer-data/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-04	Abel Womack	MA	3/9/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 1, 2016 we were notified by our Human Resources Information Systems (HRIS) provider of suspicious activity. It was determined that someone was using the HR manager's login to change the direct deposit routing and account information for Abel Womack's employees. During this process the hacker had access to the employee's name, bank routing number and bank account number. At this time it does not appear that any other personal information was accessed.

Attribution 1 Publication: NH AG's office / ME AG's office Author:
Article Title: Abel Womack
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/abel-womack-20160309.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-03	Lamps Plus / Pacific Coast Lighting	CA	2/11/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 11, 2016, an unknown criminal sent an email to an individual at Lamps Plus which was intended to look as though it came from another Lamps Plus employee. The response to that email was actually redirected to the unknown criminal and resulted in the criminal obtaining copies of your W-2 income and tax withholding statement, along with those of every other employee who worked for us during 2015.

Attribution 1 Publication: CA AG's office Author:
Article Title: Lamps Plus / Pacific Coast Lighting
Article URL: https://oag.ca.gov/system/files/Lamps%20Plus%20Notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-02	Kids Dental Care	CA	3/24/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Over the past week, KrebsOnSecurity similarly has heard from employees at a broad range of organizations that appear to have fallen victim to W2 phishing scams, including some 28,000 employees of the market research giant Kantar Group; 17,000+ employees of Sprouts Farmer's Market; call center software provider Aspect; computer backup software maker Acronis; Kids Dental Kare in Los Angeles; Century Fence, a fencing company in Wisconsin; Nation's Lending Corporation, a mortgage lending firm in Independent, Ohio; QTI Group, a Wisconsin-based human resources consulting company; and the jousting-and-feasting entertainment company Medieval Times.

Attribution 1 Publication: [krebsonsecurity.com](#) Author:
Article Title: Kids Dental Care
Article URL: <http://krebsonsecurity.com/2016/03/phishing-victims-muddle-tax-fraud-fight/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160324-01	JASACare	NY	3/14/2016	Electronic	Medical/Healthcare	Yes - Published #	1,154

JASACare, a New York-based home care services provider, has reported it has been attacked by hackers who managed to gain access to its email system. The attack is believed to have been conducted in order to steal money from corporate accounts by making fraudulent bank transfers. However, as a consequence of the breach of an employee's email account, patient and employee data was potentially compromised.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](http://hhs.gov/hipaajournal.com) Author:
Article Title: JASACARE EMAIL SYSTEM BREACH IMPACTS 1,154 PATIENTS
Article URL: <http://www.hipaajournal.com/jasacare-email-system-breach-impacts-1154-patients-3370/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160323-02	Dynamic Aviation	VA	3/18/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 11, 2016 an unidentified third party obtained access to W-2 information of all Dynamic Aviation employees for the year 2015 via an email "phishing" attack. On March 17, 2016 the fraudulent action was identified and it was determined that the information had been exposed to an unauthorized third party whose identity is presently unknown.

Attribution 1 Publication: [databreaches.net / VT AG's office](http://databreaches.net) Author:
Article Title: Dynamic Aviation
Article URL: http://www.ago.vermont.gov/assets/files/Consumer/Security_Breach/Dynamic%20Avaition%20SBN%20to%20Consum

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160323-01	CareCentrix	CT	3/21/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On March 7, 2016, we discovered that as the apparent result of a fake email from an individual impersonating a CareCentrix employee, a copy of your IRS Form W-2 was emailed to an unknown unauthorized individual on February 24, 2016.

Attribution 1 Publication: VT AG's office Author:
Article Title: CareCentrix
Article URL: http://www.ago.vermont.gov/assets/files/Consumer/Security_Breach/CareCentrix%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160322-08	Sirius XM	DC	3/17/2016	Electronic	Business	Yes - Published #	165

In February 2016, certain Sirius employees became aware that a data security incident occurred that involved a potential intrusion into the credentials of one (1) New Hampshire resident into its online accounts at SiriusXM (the "OAC"). The customer's Sirius XM customer account number, street address, email address, nickname of the customer's radio (i.e., an automobile radio) and the customer's method of payment for the SiriusXM services (i.e., credit card or check) may have been accessed.

Attribution 1 Publication: NH AG's office Author:
Article Title: Sirius XM
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/sirius-xm-20160317.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160322-07	Lanyon Solutions, Inc.	TX	3/18/2016	Electronic	Business	Yes - Unknown #	Unknown

On 10 March 2016, Lanyon was the target of a phishing email scheme that purported to be from a Lanyon executive leader and requested personal information about employees.

Attribution 1 Publication: NH AG's office Author:
Article Title: Lanyon Solutions, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/lanyon-solutions-20160318.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160322-06	eClinical Works, LLC	MA	3/7/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On February 22, 2016, as a result of a phishing email received by an eClinicalWorks employee appearing to come from a company executive, an unauthorized third party received an electronic file containing certain information on eClinicalWorks' current and former employees. The email requested employees' 2015 W-2 tax forms, which were sent to the unauthorized email account. The employee immediately realized the error and notified eClinicalWorks executives.

Attribution 1 Publication: NH AG's office Author:
Article Title: eClinical Works, LLC
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/eclinical-works-20160307.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160322-05	Complete Family Foot Care / Bizmatics	NE	3/7/2016	Electronic	Medical/Healthcare	Yes - Published #	5,883

Like many healthcare providers, our office employs the services of an independent contractor for the management and storage of electronic patient health records. We do so, in part, because doing so generally provides greater security for the information contained in those records. That information may include patient names, addresses, social security numbers, health insurance numbers, diagnoses, and treatments, but does not include credit card numbers or financial and payment information.

Attribution 1 Publication: hhs.gov / CFFC website Author:
Article Title: Complete Family Foot Care / Bizmatics
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160322-04	Illinois Valley Podiatry Group / Bizmatics	IL	3/8/2016	Electronic	Medical/Healthcare	Yes - Published #	26,588

The Illinois Valley Podiatry Group, 3322 W. Willow Knolls Drive, has announced that it has become aware of unauthorized access to its computer records, believed to have taken place last year. The names, addresses and Social Security numbers of patients may have been viewed, according to the medical office.

Attribution 1 Publication: hhs.gov / databreaches.net Author:
Article Title: Illinois Valley Podiatry Group / Bizmatics
Article URL: <http://www.databreaches.net/illinois-valley-podiatry-group-warned-26588-patients-after-contractor-hacked/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160322-03	Grand Street Medical Associates	NY	3/22/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Grand Street Medical Associates is a multi-disciplinary practice in Kingston, New York. At some point, what appears to be a vast amount of their patients' protected health information was left exposed on an unsecured FTP server. The leak was discovered by Justin Shafer, who notified GSMA and then contacted DataBreaches.net on March 12. According to data provided by Shafer and reviewed by DataBreaches.net, there were over 14,600 files and more than 20GB of data. Each file that we skimmed contained PHI on multiple patients. It appeared that the files were part of an effort to scan and digitize paper records from patients seen since December, 2011.

Attribution 1 Publication: databreaches.net Author:
Article Title: Treasure trove of Grand Street Medical Associates patient data exposed and indexed
Article URL: <http://www.databreaches.net/ny-treasure-trove-of-grand-street-medical-associates-patient-data-exposed-and-indexed/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160322-02	Sprouts	AZ	3/21/2016	Electronic	Business	Yes - Published #	21,000

Last week, a payroll department employee at the company's headquarters in Arizona responded to an email thought to be from a company senior executive. In the email, the person asked for the 2015 W-2 statements of all Sprouts workers.

Attribution 1 Publication: scmagazine.com Author:
Article Title: W-2 Data Breach places 21K Sprouts Farmers Market employees at risk
Article URL: <http://www.scmagazine.com/w-2-data-breach-places-21k-sprouts-farmers-market-employees-at-risk/article/485044/>

Attribution 2 Publication: 10news.com Author:
Article Title: Sprouts workers' payroll information exposed in fake email scam
Article URL: <http://www.10news.com/news/sprouts-workers-payroll-information-exposed-in-fake-email-scam-032116>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 190 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160322-01	ConvaTec, Inc.	NJ	3/9/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to you on behalf of my client, ConvaTec, Inc. (the "Company") and pursuant to N.H. Rev. Stat. § 359-C:20(1)(b), to inform you of a data breach. In the late evening of March 7, 2016, ConvaTec, Inc. became aware that, on February 29, 2016, a criminal impersonating a senior company official requested and received the personal information of ConvaTec employees, including their Social Security numbers.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: ConvaTec, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/convatec-20160309.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-14	Pulaski County Special School District	AR	3/19/2016	Electronic	Educational	Yes - Published #	2,602

Pulaski County Special School District leaders said Friday that personal information about all district employees dating back to January 2012 was improperly sent to a personal email account by an employee who left the district in late February. Primarily, the health insurance benefits information that is at issue in the data breach includes employee names and Social Security numbers, said Will Reid, the district's chief technology officer. But in some cases, the information included additional information about district employees.

Attribution 1 Publication: databreaches.net / arkansasonline.com Author:
Article Title: School district reports breach
Article URL: <http://www.arkansasonline.com/news/2016/mar/19/school-district-reports-breach-20160319/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-13	Springfield City Utilities	MO	3/18/2016	Electronic	Business	Yes - Published #	1,000

Federal investigators are aiding Springfield City Utilities after it fell victim to a phishing scam. City Utilities found out late Thursday that information for about 1,000 employees was obtained through the scam. Employees were alerted Friday of the incident.

Attribution 1 Publication: databreaches.net / ozarkfirst.com Author:
Article Title: Springfield City Utilities Falls Victim to Phishing Scam
Article URL: <http://www.ozarkfirst.com/news/springfield-city-utilities-falls-victim-to-phishing-scam>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-12	Moneytree	WA	3/16/2016	Electronic	Business	Yes - Unknown #	Unknown

Payday lending firm Moneytree is the latest company to alert current and former employees that their tax data — including Social Security numbers, salary and address information — was accidentally handed over directly to scam artists.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Thieves Phish Moneytree Employee Tax Data
Article URL: <http://krebsonsecurity.com/2016/03/thieves-phish-moneytree-employee-tax-data/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-11	Foss Manufacturing Company, LLC	NH	3/11/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to notify you that on March 2, 2016, Foss Manufacturing Company, LLC determined that it had been the victim of an email phishing scheme, which resulted in an unauthorized person obtaining a copy of employee 2015 W-2 forms.

Attribution 1 Publication: NH AG's office Author:
Article Title: Foss Manufacturing Company, LLC
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/foss-manufacturing-20160311.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 191 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-10	SalientCRGT	VA	3/15/2016	Electronic	Business	Yes - Published #	1,192

This letter is being sent in accordance with New Hampshire law to inform your office that our company recently suffered an email spoofing incident that resulted in an employee unwittingly sending an unknown outside third party W -2 information about one New Hampshire resident on about February 16, 2017 in response to an email request that appeared to be from a company executive. In fact the email was from an unknown outside third party. (Consumers affected per IN AG's office)

Attribution 1 Publication: NH AG's office / IN AG's office Author:
Article Title: SalientCRGT
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/salient-20150315.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-09	Sequoia Union High School District	CA	2/3/2016	Electronic	Educational	Yes - Unknown #	Unknown

On February 3, 2016, as a result of a phishing incident, an unauthorized third party accessed a SUHSD office computer and may have accessed files containing certain information on all of our employees and retirees, including myself. We can confirm that the information that may have been accessed included your name and your Social Security number. No financial or medical information was accessed.

Attribution 1 Publication: CA AG's office Author:
Article Title: Sequoia Union High School District
Article URL: https://oag.ca.gov/system/files/Sequoia%20-%20CA%20Notice%20%286003570x7AB84%29_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-08	Advance Auto Parts	VA	3/17/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 7, 2016, a third party obtained unauthorized access to employee information. This access was through a phishing-type attack in which an outside party posing as an Advance employee convinced an employee to provide a file containing information about certain individuals who worked for Advance during 2015. The employee believed the email request for this file was a legitimate internal data request.

Attribution 1 Publication: databreaches.net / CA AG's office / MT Author:
Article Title: Advance Auto Parts
Article URL: https://oag.ca.gov/system/files/ACID_PRINTPROOFS.NOTICE%20LETTER_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-07	SevOne	MA	3/14/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to inform you that on March 7, 2016, SevOne was the victim of an email phishing incident that resulted in an unauthorized disclosure of 2015 W-2 forms of current and former employees. The personal information involved included name, address, Social Security number, income information and other information found on a 2015 W-2 form.

Attribution 1 Publication: databreaches.net / NH AG's office / MD Author:
Article Title: SevOne
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/sev-one-20160314.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-06	WorkCare, Inc.	CA	2/26/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 18, 2016, as a result of a phishing incident, an unauthorized third party received an electronic file containing certain information on all current and former employees of WorkCare. Upon learning of the issue, WorkCare's incident response team promptly launched an investigation. We have confirmed that the information that was received by the unauthorized party included employees' names, Social Security numbers, home addresses, salary, and tax withholding information.

Attribution 1 Publication: NH AG's office Author:
Article Title: WorkCare, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/workcare-20160226.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 192 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-05	Lakewood Hills Internal Medicine / Felicia Lewis, MD	TX	1/14/2016	Electronic	Medical/Healthcare	Yes - Published #	1,500
Felicia Lewis, MD Lakewood Hills Internal Medicine TX Healthcare Provider 1500 01/14/2016 Hacking/IT Incident Electronic Medical Record							

Attribution 1 Publication: hhs.gov Author:
Article Title: Lakewood Hills Internal Medicine / Felicia Lewis, MD
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-04	Locust Fork Pharmacy	AL	3/9/2016	Electronic	Medical/Healthcare	Yes - Published #	5,000
Locust Fork Pharmacy in Alabama has reported a security incident to the Office for Civil Rights that has affected 5,000 of its customers. The incident is listed as an "unauthorized access/disclosure", although no further information has been made available about the incident.							

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: 5,000 Customers Affected by Locust Fork Pharmacy Data Breach
Article URL: <http://www.hipaajournal.com/almost-13000-affected-by-recent-pharmacy-data-breaches-3350/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-03	Virtua Medical Group	NJ	3/21/2016	Electronic	Medical/Healthcare	Yes - Published #	1,654
An error was made by a transcription vendor during a server upgrade that resulted in patients' names, birthdates, physicians' names, and treatment information being indexed by search engines for up to three weeks. The server error occurred in early January and the error was identified on January 21, 2016. No financial data, insurance information, or Social Security numbers were exposed.							

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: VIRTUA MEDICAL GROUP VENDOR ERROR PUTS PATIENT DATA IN SEARCH ENGINES
Article URL: <http://www.hipaajournal.com/virtua-medical-group-vendor-error-puts-patient-data-in-search-engines-3364/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-02	Office of Elliot J. Martin Chiropractic, PC	NY	2/24/2016	Electronic	Medical/Healthcare	Yes - Published #	1,200
I became aware of this potential breach on 2/19/2016. Someone may have remotely gained access to our system between 2/11/16 and 2/19/16. The information which may have been accessed could include your; name, address, social security number, date of birth, diagnosis, driver's license, credit card, laboratory findings and or other information stored on the office computer.							

Attribution 1 Publication: hhs.gov / databreaches.net Author:
Article Title: Elliot J. Martin Chiropractic notification to patients of HIPAA breach
Article URL: <http://www.databreaches.net/elliott-j-martin-chiropractic-notification-to-patients-of-hipaa-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160321-01	Centers Plan for Healthy Living	NY	3/3/2016	Electronic	Medical/Healthcare	Yes - Published #	6,893
Centers Plan for Healthy Living, a Staten Island NY-based managed care organization, has announced that a laptop computer containing the protected health information of Medicare/Medicaid recipients has been stolen from its corporate offices. The laptop theft was discovered on January 4, 2016., with the device believed to have been taken on or around January 1.							

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: 6,893 PATIENT RECORDS EXPOSED DUE TO CENTERS PLAN FOR HEALTHY LIVING LAPTOP THEFT
Article URL: <http://www.hipaajournal.com/6893-patient-records-exposed-centers-plan-for-healthy-living-laptop-theft-3360/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160318-01	PerkinElmer	AL	3/15/2016	Electronic	Business	Yes - Published #	2,738

We became aware of an incident in which an unauthorized third party was provided information regarding employees of PerkinElmer, Inc. ("PerkinElmer" or the "Company") on February 24, 2016. We began investigating the incident as soon as we became aware of the incident. Late in the afternoon on February 24, 2016, the Company discovered that a PerkinElmer employee received an email that was disguised to appear that it was sent from another Perkin Elmer employee, requesting certain employee information. The employee who received the email had access to salary and other employee information and, believing the email was legitimate, provided the requested information. At this time, we have no reason to believe that our IT systems are compromised. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: PerkinElmer
Article URL: https://oag.ca.gov/system/files/PerkinElmer%2003152016%20California%20notice%20redacted_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-15	LAZ Parking	CT	3/15/2016	Electronic	Business	Yes - Published #	14,000

The tax and revenue information for roughly 14,000 employees of the third-largest parking company in the nation, which operates in San Diego and Los Angeles, may have been stolen by an "unknown individual," the company says. LAZ, based in Hartford, Conn., said in a letter to employees that a LAZ worker was tricked by someone pretending to be an executive with the company to give up 2015 W-2 forms in mid-February by email.

Attribution 1 Publication: San Diego Union Tribue / CA AG's office Author:
Article Title: 14,000 LAZ Parking employees have data stolen
Article URL: <http://www.sandiegouniontribune.com/news/2016/mar/15/laz-parking-w2-compromise/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-14	GreenShades / Multiple entities	FL	3/9/2016	Electronic	Business	Yes - Unknown #	Unknown

The spike in tax fraud against employees of companies that use Greenshades came to light earlier this month in various media stories. A number of employees at public high schools in Chicago discovered that crooks beat them to the punch on filing tax returns. An investigation into that incident suggested security weaknesses at Greenshades were to blame. The Milwaukee Journal Sentinel wrote last month about tax fraud perpetrated against local county workers, fraud that also was linked to compromised Greenshades accounts. In Nebraska, the Lower Platte North Natural Resources District and Fremont Health hospital had a number of employees with tax fraud linked to compromised Greenshades accounts, according to a report in the Fremont Tribune.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: After Tax Fraud Spike, Payroll Firm Greenshades Ditches SSN/DOB Logins
Article URL:

Attribution 2 Publication: fox6now.com Author:
Article Title: Latest: Data breach impacting Ozaukee Co. employees didn't happen internally, locally
Article URL: <http://fox6now.com/2016/03/09/latest-data-breach-impacting-ozaukee-co-employees-didnt-happen-internally-locally/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-13	Lakes Region Scholarship Foundation	NH	3/4/2016	Electronic	Educational	Yes - Published #	2,047

Lakes Region Scholarship Foundation was contacted via telephone on February 15, 2016, by a person purporting to be calling about a computer error message. Coincidentally, the employee who answered the telephone was in the process of installing an updated version of Norton Anti-virus software and had just witnessed an error message screen. Because of this fact, the employee assumed that the call was legitimate and gave the caller access to her computer.

Attribution 1 Publication: NH AG's office / VT AG's office Author:
Article Title: Lakes Region Scholarship Foundation
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/lakes-region-scholarship-20160304.pdf>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 194 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-12	Acronis, Inc.	MA	3/4/2016	Electronic	Business	Yes - Unknown #	Unknown

On or about February 28, 2016, a sophisticated hacker was able to "spoo" our CEO's email address, meaning that the hacker was able to send an email to one of our employees that looked like it came from our CEO. The hacker's email asked for copies of employee W-2 forms. Notably, this hacker did not actually hack into our systems, and our systems were never compromised.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Acronis, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/acronis-20160304.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-11	DataXu	MA	3/3/2016	Electronic	Business	Yes - Published #	318

Please be advised that on February 18, 2016, an employee of DataXu, Inc. sent certain employee records to an unauthorized email recipient. The documents likely contained employee names, home addresses, social security numbers and salary information.

Attribution 1 Publication: NH AG's office Author:
Article Title: DataXu
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/dataxu-20160303.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-10	Endologix	CA	3/9/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Endologix was targeted by a fraudulent "phishing" email that appeared to come from an internal Endologix email address. This email was not recognized as fraudulent, and, consequently, Endologix unknowingly provided the 2015 W-2 forms of certain employees to an unauthorized third party.

Attribution 1 Publication: NH AG's office Author:
Article Title: Endologix
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/endologix-20160309.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-09	University Hospitals Geauga Medical Center	OH	3/12/2016	Electronic	Medical/Healthcare	Yes - Published #	677

A former University Hospitals employee improperly accessed medical information of 677 patients at UH Geauga Medical Center, including personal information, according to a news release from UH. The information that may have been accessed includes names, dates of birth, medical record numbers and health information related to medications.

Attribution 1 Publication: news-herald.com / databreaches.net Author:
Article Title: Information on some Geauga Medical Center patients improperly accessed
Article URL: <http://www.news-herald.com/general-news/20160310/information-on-some-geauga-medical-center-patients-improperly>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-08	MROStop LLC	NC	3/15/2016	Electronic	Business	Yes - Unknown #	Unknown

Evidence suggests that the hacker maintained limited access for a few months leading up to December 14th. During this time, the hacker accessed usernames and passwords of our customers and real-time entries of credit card information. We have been unable to identify which customers' credit card information was compromised. As soon as we discovered each component of the attack (the username/password component on December 15th and the real-time credit card component on December 14th), we immediately began working to close security vulnerabilities, eliminate redundancies in access points to our system, change all security parameters, and otherwise rectify the issue and limit risk of any future breaches. (Posted on MD AG website in 3/2016)

Attribution 1 Publication: MD AG's office / ME AG's office Author:
Article Title: MROStop LLC
Article URL: <https://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-262360.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-07	Karmanos Cancer Center	MI	3/14/2016	Electronic	Medical/Healthcare	Yes - Published #	2,808

An unencrypted flash drive containing the protected health information of 2,808 patients of the Barbara Ann Karmanos Cancer Center has been declared lost. The flash drive had been mailed to Barbara Ann Karmanos Cancer Center but when the package arrived, the flash drive was discovered to be missing.

Attribution 1 Publication: [hipaajournal.com](#) Author:
Article Title: Lost Flash Drive Exposes Data of Karmanos Cancer Center Patients
Article URL: <http://www.hipaajournal.com/lost-flash-drive-exposes-data-of-karmanos-cancer-center-patients-3353/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-06	Applied Systems	IL	3/7/2016	Electronic	Business	Yes - Published #	1,206

On February 25, 2016, Applied Systems, Inc. ("Applied") learned that an employee of the company was targeted by an email "phishing" scheme on February 19 and that the employee unfortunately, and improperly, transmitted personal information outside the company by reply email. Specifically, certain information normally found on an employee IRS Form W-2 was attached to this email, which was sent in response to what appeared to the employee to be a legitimate request from an officer of Applied for that information. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / ME AG's office / IN AG' Author:
Article Title: Applied Systems
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Applied%20Systems%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-05	Lewis Kisch and Associates Ltd.	MN	3/7/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 3, 2016, we learned that an unauthorized individual was able to gain access to certain systems of our firm. Based on our current investigation, it appears that the individual may have been able to access certain client files while on our network. We believe that the incident may have affected certain personal information contained in your tax returns, including your name, address, date of birth, phone number, Social Security number and financial account information.

Attribution 1 Publication: VT AG's office Author:
Article Title: Lewis Kisch and Associates Ltd.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Lewis%20Kisch%20and%20Associates%20Ltd%20SBN

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-04	Information Innovators Inc.	VA	3/3/2016	Electronic	Business	Yes - Unknown #	Unknown

Information Innovators Inc. ("Triple-i") recently suffered a pbisbiog attack, which resulted in the unauthorized disclosure of 2015 W-2 Forms of employees and former employees who received wages in 2015.

Attribution 1 Publication: VT AG's office / ME AG's office / NH AG' Author:
Article Title: Information Innovators Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Information%20Innovators%20Inc%20-%20Triple-i%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-03	Matrix North American Construction	IL	3/14/2016	Electronic	Business	Yes - Published #	4,650

On February 29, 2016, we and our parent company, Matrix Service Company, learned that on February 3, 2016, a targeted "spear phishing" email message had been sent to an employee of Matrix Service Company. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual." The email the employee received was designed to appear as though it had been sent to the employee from the Matrix Service Company Chief Executive Officer, requesting the names, addresses, employee identification numbers, Social Security numbers, dates of birth, and salary information for all active employees, including Matrix Service Company subsidiary companies. (Consumers affected per IN AG's office)

Attribution 1 Publication: VT AG's office / data breaches.net / IN A Author:
Article Title: Matrix North American Construction
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Matrix%20Service%20Company%20SBN%20to%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-02	Care.com	MA	3/10/2016	Electronic	Business	Yes - Unknown #	Unknown

On March 3, 2016, we became aware of a disclosure of certain 2015 Care.com payroll data to an unauthorized party, as a result of a cyberattack on March 3, 2016. The compromised information also included certain 2015 payroll information of Care.com's US based subsidiaries (Breedlove & Associates, Care Concierge and Citrus Lane). Unfortunately, a review of the data in question has determined that some of your personally identifiable information was acquired by this unauthorized party, including the following types of data: first name; last name; address; Social Security number; and 2015 salary and tax related information.

Attribution 1 Publication: VT AG's office Author:
Article Title: Care.com
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Care%20com%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160315-01	Laborers Funds Administrative Office of	CA	2/17/2016	Electronic	Business	Yes - Published #	2,373

On February 16, 2016, the Fund sent an IRS Form 1095-B to its participants confirming that they have the required minimum essential coverage from the Fund and therefore not responsible for the tax or penalty due under the Patient Protection and Affordable Care Act. On February 17, 2016, the Fund discovered that due to a computer error, a portion of the Form 1095-B documents was defective. According to the Fund's internal investigation, some of your personal information and the personal information of your dependents were included on the Form 1095-B mailed to another Fund participant.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Laborers Funds Administrative Office of Northern California, Inc.
Article URL: https://oag.ca.gov/system/files/Laborers%20Notice%20of%20Data%20Breach%20-%20Sample_0.pdf?

Attribution 2 Publication: hipaajournal.com / hhs.gov Author:
Article Title: LABORERS FUNDS ADMINISTRATIVE OFFICE OF NORTHERN CALIFORNIA REPORTS HIPAA BREACH
Article URL: <http://www.hipaajournal.com/laborers-funds-administrative-office-of-northern-california-reports-hipaa-breach-3355/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160314-02	Mitchell International, Inc.	CA	3/11/2016	Electronic	Business	Yes - Published #	1,648

On February 24, 2016, an unknown, unauthorized person from outside of Mitchell impersonated a member of Mitchell's executive leadership team and, using what appeared to be that person's legitimate Mitchell email address, convinced one of our employees to provide certain personal information about current and former employees. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: Mitchell International, Inc.
Article URL: https://oag.ca.gov/system/files/NoticeCA_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160314-01	1-800-Flowers.com	NY	3/8/2016	Electronic	Business	Yes - Unknown #	Unknown

Our customer service team received reports on February 15, 2016 from several customers that they were unable to complete their online order. Our operations team initiated an investigation and identified signs of unauthorized access to the network that operates our e-commerce platform.

Attribution 1 Publication: CA AG's office Author:
Article Title: 1-800-Flowers.com
Article URL: https://oag.ca.gov/system/files/CA%20Notification_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160308-06	GCI / General Communication, Inc.	AK	3/8/2016	Electronic	Business	Yes - Unknown #	Unknown

In an email Friday, GCI Executive Vice President Greg Chapados explained the information was accessed by someone claiming to be an employee of GCI. The individual, purporting to be GCI's chief financial officer, requested "employee payroll information, specifically copies of the W-2 Wage and Tax Statement forms for everyone who worked for GCI during calendar year 2015," Chapados wrote.

Attribution 1 Publication: Databreaches.net / KTVA / MD AG's offi Author:
Article Title: More than 2,500 General Communication, Inc. employees' W-2 information stolen in phishing scam
Article URL: <http://www.ktva.com/more-than-2500-gci-employees-w-2-information-stolen-in-phishing-scam-524/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160308-05	Adreima	IL	3/8/2016	Electronic	Business	Yes - Unknown #	Unknown

On October 12, 2015, Adreima was notified by its payroll and personnel management system vendor that earlier that day it detected suspicious changes to a number of employees' direct deposit information. Specifically, they noted that certain employees' bank account numbers and financial institution routing numbers were accessed and modified. Upon learning of this incident, Adreima worked closely with its vendor to lock down the system and terminate the unauthorized access to Adreima's account on the same day that the unauthorized access was discovered. (Posted on MD AG website in 3/2016)

Attribution 1 Publication: MD AG's office Author:
Article Title: Adreima
Article URL: <https://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260701.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160308-04	Microf LLC	GA	3/8/2016	Electronic	Business	Yes - Unknown #	Unknown

On September 30, 2015, Microf learned that an unauthorized individual may have gained access to the images uploaded to the Microf website. Upon learning th is, we immediately initiated a comprehensive internal review to safeguard our customers' information and determine what information may have been accessed. We also notified law enforcement and retained an outside computer forensic firm to assist in our investigation. Our investigation determined that the information accessed may have included name, address, date of birth, driver's license, Social Security number and other documentation related to the financing of HV AC heating and cooling systems. (Posted on MD AG website in 3/2016)

Attribution 1 Publication: MD AG's office Author:
Article Title: Microf LLC
Article URL: <https://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260746.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160308-03	Turner Construction Company	NY	3/2/2016	Electronic	Business	Yes - Published #	9,841

On March 2, 2016, certain personal information was disclosed in an email to an unauthorized recipient. We immediately began investigating and engaged third party experts to assist us with this response. Subsequently, we determined that your personally identifiable information was disclosed in this email to an unauthorized recipient. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / VT AG's office / IN AG's Author:
Article Title: Turner Construction Company
Article URL: https://oag.ca.gov/system/files/Turner%20Construction%20Ad%20r4prf_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160308-02	Blue Cross Blue Shield - South Carolina	SC	2/12/2016	Paper Data	Medical/Healthcare	Yes - Published #	998

A business associate (BA), BlueCrossBlueShield, of the covered entity (CE), South Carolina Public Employee Benefit Authority, incorrectly mailed pre-authorization dental letters to the CE's members due to a computer error. During the mailing sorting process, the names of the envelopes were not matched to the correct addresses. The breach affected 998 individuals and included financial, demographic, and clinical information. The BA provided breach notification to HHS, affected individuals, and the media.

Attribution 1 Publication: hhs.gov Author:
Article Title: Blue Cross Blue Shield - South Carolina
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160308-01	Premier Healthcare	IN	3/8/2016	Electronic	Medical/Healthcare	Yes - Published #	205,748

Premier Healthcare employees discovered that the laptop was stolen from the Billing Department in its locked and alarmed administrative office on January 4. The laptop was password-protected, but was not encrypted. Emails stored on the hard drive on that laptop contained some screenshots, spreadsheets, and pdf documents that were used to address billing issues with patients, insurance companies, and other healthcare providers.

Attribution 1 Publication: cbs4indy.com Author:
Article Title: Premier Healthcare reports possible data breach after laptop is stolen
Article URL: <http://cbs4indy.com/2016/03/08/premier-healthcare-reports-possible-data-breach-after-laptop-is-stolen/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160307-09	Luzerne County Community College	PA	3/3/2016	Electronic	Educational	Yes - Unknown #	Unknown

College officials admit more than 300 faculty and staff members had their Social Security numbers sent out to each other Wednesday afternoon. The mistake left administrators scrambling to limit the damage. School officials say an email from the comptroller's office accidentally contained an attachment that had the Social Security numbers of faculty and staffers matched to their names.

Attribution 1 Publication: wnep.com Author:
Article Title: Security Breach at Luzerne County Community College
Article URL: <http://wnep.com/2016/03/03/security-breach-at-luzerne-county-community-college/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160307-08	Mansueto Ventures Inc. / Fast Company magazines	NY	3/4/2016	Electronic	Business	Yes - Unknown #	Unknown

Mansueto Ventures, publisher of Inc. and Fast Company magazines, was the victim of a massive data breach that exposed employees' wage information and Social Security numbers to hackers.

Attribution 1 Publication: nypost.com Author:
Article Title: Hackers victimize Inc., Fast Company staffers
Article URL: <http://nypost.com/2016/03/04/hackers-victimize-inc-fast-company-staffers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160307-07	Seagate	CA	3/6/2016	Electronic	Business	Yes - Published #	8,292

Email scam artists last week tricked an employee at data storage giant Seagate Technology into giving away W-2 tax documents on all current and past employees, KrebsOnSecurity has learned. W-2 forms contain employee Social Security numbers, salaries and other personal data, and are highly prized by thieves involved in filing phony tax refund requests with the Internal Revenue Service (IRS) and the states. (Consumers affected per IN AG's office)

Attribution 1 Publication: krebsonsecurity.com / CA AG's office / I Author:
Article Title: Seagate Phish Exposes All Employee W-2's
Article URL: <http://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/>

Attribution 2 Publication: zdnet.com Author:
Article Title: Seagate sued by angry staff following phishing data breach
Article URL: <http://www.zdnet.com/article/seagate-sued-by-angry-staff-following-phishing-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160307-06	City of Hope Hospital	CA	3/7/2016	Electronic	Medical/Healthcare	Yes - Published #	1,024

A phishing attack on California's City of Hope Hospital has resulted in four staff email accounts being compromised. Three out of the four compromised email accounts contained a limited amount of protected health information, although the hospital does not believe the attack took place with a view to obtaining patient data.

Attribution 1 Publication: [hipaajournal.com](#) Author:
Article Title: Staff Email Accounts Compromised in City of Hope Hospital Phishing Attack
Article URL: <http://www.hipaajournal.com/email-accounts-compromised-city-of-hope-hospital-phishing-attack-3344/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160307-05	Department of Human Services - Iowa	IA	3/7/2016	Electronic	Government/Military	Yes - Published #	425

The HIPAA breach occurred in December 2015, although it was not discovered by Iowa DHS until January 22, 2016. The privacy breach occurred when Iowa DHS' Medicaid Enterprise Medical Services department sent roster reports to the nursing homes. Those reports contained the names, Medicaid identification numbers, insurance or government program information, and the facility where each patient currently resides.

Attribution 1 Publication: [hipaajournal.com](#) Author:
Article Title: Nursing Home Residents' PHI Accidentally Disclosed by Iowa DHS
Article URL: <http://www.hipaajournal.com/nursing-home-residents-phi-disclosed-iowa-dhs-3345/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160307-04	21st Century Oncology	FL	3/7/2016	Electronic	Medical/Healthcare	Yes - Published #	2,213,597

In October, a hacker gained access to a patient database at 21st Century Oncology containing insurance data and Social Security numbers of patients. The incident is not of the order of the breaches at Anthem, Excellus BCBS, or Primera Blue Cross, but it does rank as one of the largest healthcare data breaches of 2015. On March 4, 2016, a regulatory filing was issued to the United States Securities and Exchange Commission indicating 2.2 million current and former patients were affected and potentially had their data copied and stolen.

Attribution 1 Publication: [hipaajournal.com / CA AG's office / SC](#) Author:
Article Title: 21st Century Oncology Advises 2.2M Patients of Hacking Incident
Article URL: <http://www.hipaajournal.com/21st-century-oncology-2-2-million-hacking-incident-3346/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160307-03	Freepoint Memorial Hospital	IL	2/26/2016	Electronic	Medical/Healthcare	Yes - Published #	1,349

Freepoint Memorial Hospital (FHN) recently announced that on December 30, 2015, a computer hard drive containing patient information was stolen from an FHN employee's office that was in a "secure nonpublic area." The hard drive contained internal reports and spreadsheets with patient data. The information potentially exposed includes names, phone numbers, addresses, dates of birth, ethnicity, email addresses, medical record numbers, FHN patient identification numbers, patient encounter numbers, Social Security numbers, dates of service, procedures, billing codes, examinations, diagnoses, names of physicians, health insurance information, medication information, and dates of discharge.

Attribution 1 Publication: [hhs.gov / healthitsecurity.com](#) Author:
Article Title: Hard drive stolen at Illinois hospital
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160307-02	Roark's Pharmacy	TN	2/19/2016	Electronic	Medical/Healthcare	Yes - Published #	2,393

A hard drive containing customer prescription information and personal data was stolen by thieves who broke in to the pharmacy in the early hours of January 13. The break-in and theft was discovered four hours later when pharmacy owner, Terry Roark, arrived to open the store at 6:30am.

Attribution 1 Publication: [hhs.gov / hipaajournal.com](http://hhs.gov/hipaajournal.com) Author:
Article Title: Hard Drive Containing 3000 Customers' PHI Stolen in Roark's Pharmacy Burglary
Article URL: <http://www.hipaajournal.com/almost-13000-affected-by-recent-pharmacy-data-breaches-3350/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160307-01	Public Health Trust of Miami-Dade, FL	FL	2/19/2016	Electronic	Medical/Healthcare	Yes - Published #	24,188
Public Health Trust of Miami-Dade County, Florida FL Healthcare Provider 24188 02/19/2016 Unauthorized Access/Disclosure Electronic Medical Record							

Attribution 1 Publication: hhs.gov Author:
Article Title: Public Health Trust of Miami-Dade, FL
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160304-03	Billy Casper Golf	VA	3/3/2016	Electronic	Business	Yes - Published #	8,176
On Friday, February 26, Billy Casper Golf was the targeted victim of an e-mail spoofing attack. Through this attack, a request was made for all 2015 employee W2 information. Unfortunately, this information was provided before it was discovered that the request was made from a fraudulent account by an individual purporting to be our CEO. We discovered the fraudulent nature of this request on Saturday, February 27, 2-16 and have been working tirelessly to investigate. (Consumers affected per IN AG's office)							

Attribution 1 Publication: VT AG's office / IN AG's office Author:
Article Title: Billy Casper Golf
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Billy%20Casper%20Golf%20SBN%20to%20Consumers

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160304-02	Evening Post Industries	SC	3/3/2016	Electronic	Business	Yes - Published #	2,314
On Friday, February 26, 2016, Evening Post Industries was the targeted victim of an email spoofing incident. Through this incident, a request was made for a summary of all 2015 employee W2 information - to include all affiliates. Unfortunately this information was provided before we discovered that the request was made from a fraudulent account, by an individual purporting to be John Barnwell. (Consumers affected per IN AG's office)							

Attribution 1 Publication: VT AG's office / NH AG's office / IN AG's Author:
Article Title: Evening Post Industries
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Evening%20Post%20Industries%20SBN%20to%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160304-01	Rosen Hotels and Resorts	FL	3/4/2016	Electronic	Business	Yes - Unknown #	Unknown
We received unconfirmed reports on February 3, 2016 of a pattern of unauthorized charges occurring on payment cards after they had been used by some of our guests during their stay. Findings from the investigation show that an unauthorized person installed malware in RH&R's payment card network that searched for data read from the magnetic stripe of payment cards as it was routed through the affected systems. In some instances the malware identified payment card data that included cardholder name, card number, expiration date, and internal verification code.							

Attribution 1 Publication: CA AG's office / rosenhotels.com Author:
Article Title: Rosen Hotels & Resorts Inc. Completes Investigation of Payment Card Incident
Article URL: <http://www.rosenhotels.com/protectingourguests/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-10	Actifio, Inc.	MA	3/2/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing on behalf of my client, Actifio, Inc. (Actifio), to notify you that on February 16, 2016, my client became aware that a spreadsheet with Actifio payroll data was acquired by an unauthorized party on or about February 3, 2016, as a result of a phishing attack targeted at Actifio.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Actifio, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/actifio-20160302.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-09	AmeriPride Services, Inc.	MN	2/26/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 25, 2016, a third party fraudulently obtained employee W2 forms from AmeriPride by using an email that was disguised to appear as if it was from an internal employee. The W2s contain information including names and addresses, social security numbers, wages, withholdings and marital statuses. Other personally identifiable information (bank account numbers, PIN, security codes) was not compromised.

Attribution 1 Publication: NH AG's office Author:
Article Title: AmeriPride Services, Inc.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/ameripride-20160226.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-08	Illinois State University	IL	3/2/2016	Electronic	Educational	Yes - Unknown #	Unknown

An apparent information breach at Illinois State University allowed someone to divert the direct-deposit payroll payments of more than a dozen faculty and staff members to another account, according to university officials.

Attribution 1 Publication: pekintimes.com Author:
Article Title: Data breach targets Illinois State University payroll
Article URL: <http://www.pekintimes.com/news/20160302/data-breach-targets-illinois-state-university-payroll>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-07	Cox Communications	GA	3/3/2016	Electronic	Business	Yes - Unknown #	Unknown

Apparent names, email addresses, phone numbers, and other information relating to some 40,000 Cox Communications employees is currently advertised on a marketplace specialising in stolen data and computer exploits.

Attribution 1 Publication: motherboard.vice.com Author:
Article Title: Cox Investigates as Employee Data Appears for Sale on the Dark Web
Article URL: <http://motherboard.vice.com/read/cox-investigates-as-employee-data-appears-for-sale-on-the-dark-web>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-06	Wal-Mart Stores, Inc. (Pharmacy)	AR	3/3/2016	Electronic	Medical/Healthcare	Yes - Published #	4,800

Wal-Mart Stores Inc said on Wednesday that prescription history and other basic information on a few thousand online U.S. pharmacy customers may have been visible to other users during a four-day stretch last month due to a coding mistake.

Attribution 1 Publication: databreaches.net / Reuters.com / hipaaj Author:
Article Title: Wal-Mart says some pharmacy client data was visible to others online
Article URL: <http://www.reuters.com/article/walmart-pharmacy-idUSL2N16A1N3>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-05	Nintendo Health Plan / Premera	WA	3/3/2016	Electronic	Medical/Healthcare	Yes - Published #	6,248

The covered entity (CE), Nintendo of America, Inc., reported that on May 5, 2014, attackers impermissibly accessed and acquired data in possession of its business associate (BA), Premera. This data included the protected health information (PHI) of former and current participants in health plans of certain members of the Blue Cross Blue Shield Association dating back to 2002. The BA is a member of the Blue Cross Blue Shield Association and is the third-party administrator for the health plan. As a result, some former and current plan participants have been impacted. The CE reported that 6,248 individuals were affected and the PHI involved in the breach included demographic, clinical, and financial information.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Nintendo Health Plan breach impacts 6,248
Article URL: <http://www.databreaches.net/nintendo-health-plan-breach-impacts-6248/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-04	Main Line Health	PA	3/3/2016	Electronic	Medical/Healthcare	Yes - Published #	11,000

Main Line Health has fallen victim to a spear phishing attack that has resulted in the data of employees being sent to a scammer. This is the fourth such case discovered in the past two weeks that has resulted in a breach of employee data. The spear phishing attack was discovered on Tuesday this week, although the spear phishing email was sent to a Main Line Health employee on February 16, 2016.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: INVESTIGATION LAUNCHED INTO MAIN LIFE HEALTH SPEAR PHISHING ATTACK
Article URL: <http://www.hipaajournal.com/main-life-health-spear-phishing-attack-3340/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-03	Eye Institute of Corpus Christi / Dr. Ravi Krishnan	TX	3/3/2016	Electronic	Medical/Healthcare	Yes - Published #	43,961

The Eye Institute of Corpus Christi, a full service eye care, diagnosis, and treatment clinic in Texas, has discovered that individuals gained access to the records of all of its patients, downloaded their protected health information from the EHR, copied those data, and provided them to two physicians formerly employed by the eye clinic. The disclosed data include the names of patients, their addresses, contact telephone numbers, Social Security numbers, dates of birth, medical diagnoses, details of treatment, and health insurance details.

Attribution 1 Publication: hipaajournal.com / NH AG;s office Author:
Article Title: DATA BREACH DISCOVERED BY THE EYE INSTITUTE OF CORPUS CHRISTI
Article URL: <http://www.hipaajournal.com/data-breach-discovered-by-the-eye-institute-of-corpus-christi-3341/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-02	Robert Rauschenberg Foundation	NY	2/25/2016	Electronic	Business	Yes - Unknown #	Unknown

On or about January 25, 2016, RRF learned it had been the victim of a phishing attack. The phishing attack allowed an unknown individual or individuals access into an RRF email account, where the unknown individual or individuals may have had access to personally identifiable information on individuals contained within the email account. The potential unauthorized access began on January 23, 2016 and ended on January 25, 2016. This notice has not been delayed as a result of a law enforcement investigation.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Robert Rauschenberg Foundation
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Robert%20Rauschenberg%20Foundation%20SBN%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160303-01	Pharm-Olam International	TX	2/25/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 23, 2016, due to a security incident, your 2015 W-2 form was disclosed to an unauthorized recipient. The W-2 form includes your name, address, Social Security number, and 2015 wage information. This incident is being internally investigated. We also immediately notified law enforcement and appropriate authorities/entities, and are cooperating with their concurrent investigation.

Attribution 1 Publication: VT AG's office Author:
Article Title: Pharm-Olam International
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Pharm-Olam%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160302-01	Central Concrete Supply Co.	CA	3/2/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 24, 2016, we became aware of a data breach by which we believe a third party obtained access to copies of your 2015 W-2 income and tax withholding statements. This information was stolen through a sophisticated social engineering scheme in which an outside party posing as another person convinced an employee of Central Concrete Supply to provide copies of the documents by email on February 23, 2016. The data was not obtained through any breach of the Company's information technology systems.

Attribution 1 Publication: CA AG's office Author:
Article Title: Central Concrete Supply Co.
Article URL: https://oag.ca.gov/system/files/Central%20Concrete%20Ad%20r1fin_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160301-05	FHN Memorial Hospital	IL	2/29/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A computer hard drive containing patient information was stolen from FHN Memorial Hospital in December. The hard drive did not contain medical records, but did have internal reports and spreadsheets with patient data, according to a FHN news release. The files may have included a patient's name, Social Security number, contact information, birthday, ethnicity, medical record number, patient ID numbers, unique patient encounter number, date of service and description of the procedure, type of examination and diagnoses, name of physician, insurance provider, medication information and date of discharge.

Attribution 1 Publication: databreaches.net / rrstar.com Author:
Article Title: FHN patient information compromised in hard drive theft
Article URL: <http://www.rrstar.com/news/20160226/fhn-patient-information-compromised-in-hard-drive-theft>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160301-04	Montgomery County School System / WestEd	DC	3/1/2016	Electronic	Educational	Yes - Unknown #	Unknown

A contractor working with the Montgomery County school system has informed the parents of about 340 special-education students that the children's private data was on a computer stolen during a break-in. WestEd officials say the data was on the hard drive of a laptop that was stolen Nov. 3, when intruders broke into the organization's D.C. offices and carted off five computers.

Attribution 1 Publication: databreaches.net / washingtonpost.com Author:
Article Title: Stolen computer had special-education student data on hard drive
Article URL: <https://www.washingtonpost.com/local/education/stolen-computer-had-special-education-student-data-on-hard-drive/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160301-03	Snapchat	CA	2/29/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 26, the company says, an email claiming to come from the CEO and asking for payroll data was sent to Snapchat's payroll department. "Unfortunately, the phishing email wasn't recognized for what it was -- a scam -- and payroll information about some current and former employees was disclosed externally."

Attribution 1 Publication: esecurityplanet.com / CA AG's office Author:
Article Title: Snapchat Breached by Spear Phishing Attack
Article URL: <http://www.esecurityplanet.com/network-security/snapchat-breached-by-spear-phishing-attack.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160301-02	TN Marketing	MN	3/1/2016	Electronic	Business	Yes - Published #	13,118

On or around January 13, 2016, TN Marketing discovered evidence of a potential vulnerability in the code used for the checkout pages of the e-commerce pages managed by TN Marketing. We moved quickly to investigate this vulnerability after it was discovered and to determine what, if any, impact this vulnerability had on our customers. Third party forensic investigators were retained to assist with the investigation. (Consumers affected per IN AG's office)

Attribution 1 Publication: CA AG's office / IN AG's office Author:
Article Title: TN Marketing
Article URL: https://oag.ca.gov/system/files/TN%20Marketing%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160301-01	BJC Healthcare ACO, LLC	MO	2/26/2016	Electronic	Medical/Healthcare	Yes - Published #	2,393

BJC HealthCare, a not-for-profit health system based in St. Louis, MO., has started notifying 2,393 of its patients that some of their protected health information has been exposed as a result of an email error that occurred on December 30, 2015.

Attribution 1 Publication: [hhs.gov / hipaajournal.com / healthitsec](http://hhs.gov/hipaajournal.com/healthitsec) Author:
Article Title: BJC Healthcare ACO, LLC
Article URL: <http://www.hipaajournal.com/hipaa-breaching-email-exposed-bjc-healthcare-patients-data-8334/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160229-01	Vancouver Radiologists	WA	2/26/2016	Electronic	Medical/Healthcare	Yes - Published #	603

The postcards were mailed to patients at their addresses but with another patient's name on the label. The postcards included the incorrect patient name, the name of Vancouver Radiologists and a reminder that it was time to schedule an annual mammogram.

Attribution 1 Publication: [databreaches.net / columbian.com](http://databreaches.net/columbian.com) Author:
Article Title: Medical office mistakenly reveals patient names
Article URL: <http://www.columbian.com/news/2016/feb/26/medical-office-mistakenly-reveals-patient-names/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160226-05	Office of Allen Park, Attorney	MI	2/26/2016	Paper Data	Business	Yes - Unknown #	Unknown

It's common knowledge documents with personal information should be destroyed after no longer needed in order to lessen chances of identity theft. In most cases they're put through a shredder. That wasn't the case last Sunday when a man using the Wyandotte Recycling Center, came upon documents that raised all sorts of red flags. "I just found tons of personal court documents like bankruptcy files, wills and power of attorney papers, along with birth and death certificates," "It looks like someone emptied all of the files to get recycled and for the public to see. This stuff could cause a lot of trouble in the right hands."

Attribution 1 Publication: thenewsherald.com Author:
Article Title: Resident discovers sensitive personal documents in Wyandotte Recycling Center bin
Article URL: <http://www.thenewsherald.com/articles/2016/02/26/news/doc56cf9fe74ff70300485947.txt?viewmode=fullstory>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160226-04	Valley Hope Association	KS	2/26/2016	Electronic	Medical/Healthcare	Yes - Published #	52,076

On December 30, 2015, a Valley Hope Association employee had her work-issued laptop stolen from her vehicle. The laptop was password protected. The theft of the laptop was discovered on December 30, 2015, and immediately reported to local law enforcement. This notice has not been delayed at the request of law enforcement. However, law enforcement is actively investigating this matter and Valley Hope Association is cooperating in the ongoing criminal investigation. To date, there have been no arrests relating to the theft nor has the laptop been recovered.

Attribution 1 Publication: [databreaches.net / VHA website / healthi](http://databreaches.net/vha-website/healthi) Author:
Article Title: Laptop with sensitive personal and medical info stolen from Valley Hope Association employee's car
Article URL: <http://www.databreaches.net/ks-laptop-with-sensitive-personal-and-medical-info-stolen-from-valley-hope-association->

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160226-03	Coast Central Credit Union	CA	2/25/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Notifying people and companies about data breaches often can be a frustrating and thankless job. Despite my best efforts, sometimes a breach victim I'm alerting will come away convinced that I am not an investigative journalist but instead a scammer. This happened most recently this week, when I told a California credit union that its online banking site was compromised and apparently had been for nearly two months.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Breached Credit Union Comes Out of its Shell
Article URL: <https://krebsonsecurity.com/2016/02/breached-credit-union-comes-out-of-its-shell/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160226-02	University of California Berkeley	CA	2/26/2016	Electronic	Educational	Yes - Published #	80,000

On December 28, 2015 an unauthorized person or persons accessed portions of computer systems that are part of the UC Berkeley financial system. The criminals gained entry through a security flaw that the University was in the process of patching. Law enforcement, including the FBI, has been notified.

Attribution 1 Publication: dailycal.org / CA AG's office Author:
Article Title: Campus notifies nearly 80,000 students, staff regarding possible security breach
Article URL: <http://www.dailycal.org/2016/02/26/campus-notifies-nearly-80000-students-staff-regarding-possible-security-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160226-01	Sterbick & Associates, P.S.	WA	2/26/2016	Electronic	Business	Yes - Unknown #	Unknown

On August 23, 2015, our office was burglarized in which a computer CPU was stolen. It was reported to the Tacoma Police Department, case No. 15-235-1172. This computer had been in use since 2010 and was loaded with software to process tax returns and run IRS compliance checks for our tax, IRS, and bankruptcy clients. It therefore may contain personal information, including Social Security numbers, of every client since 2010. (Breach notifications now available on WA AG's website)

Attribution 1 Publication: WA AG's office Author:
Article Title: Sterbick & Associates, P.S.
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/Sterbick_Associate

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160225-04	Mercy Housing, Inc. / Mercy Housing Management Group,	CO	2/7/2016	Electronic	Business	Yes - Unknown #	Unknown

As those of you we were able to reach by email know, late Friday afternoon there was an unauthorized release of an electronic copy of all 2015 W2s issued by Mercy Housing's payroll department due to an email scam. As a result, unauthorized individuals may have personal information about you. This is a security breach of personal information.

Attribution 1 Publication: CA AG's office Author:
Article Title: Mercy Housing, Inc. / Mercy Housing Management Group, Inc.
Article URL: https://oag.ca.gov/system/files/Employee%20Letter%202015%2002%2022_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160225-03	Rightside	WA	2/25/2016	Electronic	Business	Yes - Unknown #	Unknown

Kirkland-based Rightside (Nasdaq: NAME) was the target of a "highly sophisticated phishing scam," resulting in the theft of employees' personal information, according to an email obtained by the Puget Sound Business Journal. The company notified affected employees this week, explaining that it had been the target of a cyber attack for several months and, on Tuesday, W-2 forms from current and past employees had been stolen. Rightside confirmed the data breach on Thursday.

Attribution 1 Publication: databreaches.net / bizjournals.com Author:
Article Title: Exclusive: Rightside employee tax information stolen in data breach
Article URL: <http://www.bizjournals.com/seattle/blog/techflash/2016/02/exclusive-rights-side-employee-tax-information.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160225-02	Bay Area Chiropractic Center	OR	2/24/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

According to the notification letter to patients, BACC discovered that a substitute doctor who had been working for them had acquired patients' personal information, including names, addresses, and telephone numbers for unauthorized purposes.

Attribution 1 Publication: databreaches.net Author:
Article Title: Bay Area Chiropractic Center patient info allegedly stolen by doctor to open his own practice
Article URL: <http://www.databreaches.net/bay-area-chiropractic-center-patient-info-allegedly-stolen-by-doctor-to-open-his-own-pra>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160225-01	York Hospital	ME	2/24/2016	Electronic	Medical/Healthcare	Yes - Published #	1,400

York Hospital has been hit by cyber criminals who stole identifying information from employees, but the hospital says patient information was not targeted.

Attribution 1 Publication: databreaches.net / seacoastonline.com / Author:
Article Title: Data breach hits York Hospital employees
Article URL: <http://www.seacoastonline.com/news/20160224/data-breach-hits-york-hospital-employees>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160224-01	Jacksonville State University	AL	2/23/2016	Electronic	Educational	Yes - Unknown #	Unknown

Jacksonville State University officials learned Tuesday of a website that allows users to search for students' personal information, including photos, addresses and phone numbers, all apparently stolen from JSU's own database. The site allows visitors to search using students' names to find photographs along with birthdates, student ID numbers, fraternity and sorority affiliation and other information. Information for some former students, faculty and staff is also on the site.

Attribution 1 Publication: annistonstar.com Author:
Article Title: Site posts personal info of JSU students, faculty
Article URL: http://www.annistonstar.com/news/site-posts-personal-info-of-jsu-students-faculty/article_858bcf2c-da86-11e5-9de5-6f

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160223-04	Incipio, LLC	CA	1/29/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 4, 2016, while timely installing an application software update to our e-commerce platform, we discovered that an unauthorized party had gained access to one of our cloud-based website servers. Despite our robust controls to protect you from the nefarious efforts of hackers, our investigation reveals that the unauthorized party gained access to personal information of customers who purchased product from www.incipio.com between September 26, 2015, and January 29, 2016.

Attribution 1 Publication: CA AG's office / MT AG's office Author:
Article Title: Incipio, LLC
Article URL: https://oag.ca.gov/system/files/Incipio%20Ad%20r2prf_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160223-03	EWTN Global Catholic Network	AL	2/23/2016	Electronic	Business	Yes - Published #	425

"On Friday evening, February 19, EWTN became aware of a data breach by which we believe a third party obtained access to copies of the 2015 W-2 income and tax withholding statements for all EWTN employees in the United States. Those copies included social security numbers and other personal information for each person employed by EWTN in 2015. Approximately 425 individuals in 25 states are affected. This information was gained through what is commonly known as a 'social engineering' scheme. An outside party posing as another person was able to convince an employee of EWTN to provide copies of the documents by email.

Attribution 1 Publication: al.com / krebsonsecurity.com Author:
Article Title: EWTN reports security breach of 425 employees' data by scam
Article URL: http://www.al.com/living/index.ssf/2016/02/ewtn_reports_security_breach_o.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160223-02	United Medical / Lincare Inc.	FL	2/3/2016	Paper Data	Medical/Healthcare	Yes - Published #	278

The investigation by OCR confirmed that PHI had been removed from Lincare facilities, exposed to an individual unauthorized to view PHI, and that the Lincare employee had abandoned the documents. Further, the investigation revealed a number of HIPAA violations.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Lincare Inc to Pay \$239,800 CMP for HIPAA Violation
Article URL: <http://www.hipaajournal.com/lincare-inc-ordered-to-pay-239000-cmp-for-hipaa-violation-8296/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160223-01	Saint Joseph's Healthcare System	NJ	2/23/2016	Electronic	Medical/Healthcare	Yes - Published #	5,924

A Passaic County hospital says that a security breach caused some personal information about some of its employees to get out. Saint Joseph's Healthcare System in Paterson says that a phishing scam has led to the unintentional disclosure of employee information, including Social Security numbers. (Consumers affected per IN AG's office)

Attribution 1 Publication: databreaches.nets / News12.com / IN A Author:
Article Title: St. Joseph Hospital employee information leaked in security breach
Article URL: <http://newjersey.news12.com/news/saint-joseph-s-healthcare-system-employee-information-leaked-in-security-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160222-03	Rite Aid Store #01617	NY	2/3/2016	Electronic	Medical/Healthcare	Yes - Published #	976

Rite Aid Store 01617 NY Healthcare Provider 976 02/03/2016 Unauthorized Access/Disclosure Desktop Computer, Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Rite Aid Store #01617
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160222-02	DataStat, Inc.	MI	2/12/2016	Paper Data	Medical/Healthcare	Yes - Published #	552

An employee of a business associate (BA), DataStat, erroneously misdirected surveys to 487 individuals after failing to following the BA's re-print protocol after a printer paper jam. The types of protected health information (PHI) involved in the breach included demographic information, including names and addresses. The CE provided breach notification to HHS and affected individuals. The BA also improved technical safeguards to assist with quality assessment checks and sanctioned the involved employee with a written warning. OCR obtained documentation that the BA implemented the corrective actions steps listed above.

Attribution 1 Publication: hhs.gov Author:
Article Title: DataStat, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160222-01	uKnowKids	VA	2/22/2016	Electronic	Business	Yes - Published #	1,740

A misconfigured database from a child tracking & monitoring firm exposed over 6.8 million private child text messages, 1.8 million images (many depicting children), and over 1700 in-depth child profiles.

Attribution 1 Publication: databreaches.net Author:
Article Title: uKnowKids database exposed personal and location info of 1,740 kids
Article URL: <http://www.databreaches.net/uknowkids-database-exposed-personal-and-location-info-of-1740-kids/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160218-03	IRS	DC	2/10/2016	Electronic	Government/Military	Yes - Published #	101,000

Attackers using malware and stolen personal information managed to generate 101,000 e-filing PIN numbers, according to the IRS. Affected taxpayers will be notified by mail, and their accounts will be monitored.

Attribution 1 Publication: digitaltrends.com Author:
Article Title: Identity thieves used thousands of stolen SSNs to generate IRS e-filing pins
Article URL: <http://www.digitaltrends.com/computing/identity-theft-taxes-irs-hacked/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160218-02	Shire Human Genetic Therapies	MA	2/17/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On December 30, 2015, a laptop issued by Shire Human Genetic Therapies, Inc. was stolen from the car of an employee of a Shire company. The theft occurred in Washington, D.C., and the employee immediately reported it to local law enforcement. Upon receiving notice of the theft, we promptly initiated steps to evaluate the contents of the laptop. Subsequently, after identifying and analyzing a backup copy of the laptop, we determined that the stolen laptop contained some of your personal information, which may have included your name, date of birth, address, telephone number, the last four digits of your social security number, dates of treatment, description of medical condition, and the therapeutic drug you may have used.

Attribution 1 Publication: VT AG's office / ME AG's office / MT AG' Author:
Article Title: Shire Human Genetic Therapies
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Shire%20Human%20Genetic%20Therapies%20SBN%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160218-01	Polycom	CA	2/12/2016	Electronic	Business	Yes - Unknown #	Unknown

On February 5, 2016, Polycom was the target of a phishing email that resulted in the unauthorized acquisition by a third party of certain employee information. The employee information consisted of names, addresses, Social Security numbers, dates of birth, and base salary information.

Attribution 1 Publication: VT AG's office / MT AG's office Author:
Article Title: Polycom
Article URL: [On February 5, 2016, Polycom was the target of a phishing email that resulted in the unauthorized acquisition by a thir](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160217-02	Calpine Corporation	TX	2/9/2016	Electronic	Business	Yes - Unknown #	Unknown

We learned from law enforcement that the car that was broken into is one of several cars broken into on the same day, in the same general vicinity. We believe that the theft was likely conducted by someone interested in the value of hardware stolen as opposed to information or files on the computer. In addition, the computer was password protected and contained software that would cause the computer to be immediately wiped if the unauthorized user connected to the Internet. Also, the financial information on the laptop was maintained in a format that would make it difficult for a bad actor to exploit.

Attribution 1 Publication: CA AG's letter / ME AG's office Author:
Article Title: Calpine Corporation
Article URL: <https://oag.ca.gov/ecrime/databreach/reports/sb24-60083>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160216-05	Dallas County	TX	2/15/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

Your social security number—and your child's— may have been exposed on a government website for more than decade. The CBS I-Team discovered A major security breach involving tens of thousands of North Texans. And, as shocking as the information being out there, is how long I-Team Senior Investigative Reporter Ginger Allen had to pressure Dallas County to fix the problem.

Attribution 1 Publication: dfw.cbslocal.com Author:
Article Title: I-Team Investigation Reveals Massive Security Breach In Dallas County
Article URL: <http://dfw.cbslocal.com/2016/02/15/i-team-investigation-reveals-massive-security-breach-in-dallas-county/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160216-04	Vidant Health	NC	2/16/2016	Electronic	Medical/Healthcare	Yes - Published #	897

"Vidant Health discovered that personal information for Vidant Duplin Hospital employees was subject to unauthorized access by an outside source. The unauthorized access occurred in early February. We notified employees in writing and meetings. Vidant has controls surrounding employees' information. These controls worked to discover the unintended access and avoided additional information disclosure.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Vidant Health notified employees of data breach
Article URL: <http://www.databreaches.net/nc-vidant-health-notified-employees-of-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160216-03	Kankakee Valley REMC (Rutherford Electric)	IN	2/16/2016	Electronic	Business	Yes - Published #	17,700

According to a press release issued by the electric utility cooperative, the breach was detected by an audit in mid-January that indicated that a foreign IP address had accessed a storage device on the network.

Attribution 1 Publication: databreaches.net Author:
Article Title: Security breach reported by Kankakee Valley REMC
Article URL: <http://www.databreaches.net/in-security-breach-reported-by-kankakee-valley-remc/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160216-02	Magnolia Health Corporation	CA	2/12/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On February 3, 2016 an unidentified third person impersonated our CEO, Kenny Moyle, and using what appeared to be his email address, obtained certain personal information for all active employees of Magnolia Health Corporation (MHC) and each of the facilities managed by MHC [Twin Oaks Assisted Living, Inc., Twin Oaks Rehabilitation And Nursing Center, Inc., Porterville Convalescent, Inc., Kaweah Manor, Inc. and Merritt Manor, Inc.].

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Mississippi's Magnolia Health Fires Employee for PHI Disclosure
Article URL: <http://www.hipaajournal.com/mississippis-magnolia-health-fires-employee-for-phi-disclosure-8326/>

Attribution 2 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Magnolia Health Victim of Spoofed Email Phishing Scam
Article URL: <http://www.hipaajournal.com/magnolia-health-victim-of-email-spoofing-phishing-scam-8314/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160212-03	DC Public School District	DC	2/11/2016	Electronic	Educational	Yes - Published #	12,000

The private information of about 12,000 D.C. Public Schools students was accidentally uploaded to a publicly accessible website, the District's Office of the State Superintendent of Education announced Thursday in an internal memo. The information included each student's identification number, race, age, school, disabilities and any services he or she receives.

Attribution 1 Publication: washingtonpost.com / databreaches.net Author:
Article Title: D.C. accidentally uploads private data of 12,000 students
Article URL: <https://www.washingtonpost.com/local/education/dc-accidentally-uploads-private-information-of-12000-students/2016/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160212-02	University of Texas System Administration	TX	1/21/2016	Electronic	Educational	Yes - Published #	794

The University of Texas System Administration TX Health Plan 794 01/21/2016 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: University of Texas System Administration
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160211-05	Oregon Health & Science University	OR	2/11/2016	Electronic	Educational	Yes - Unknown #	Unknown

On December 6, 2015, an OHSU research student's car was broken into and a hard drive was stolen. The hard drive may have contained health information about Neonatal Intensive Care Unit patients admitted to the unit in 2013 who were enrolled in a research study about the potential effect of aminoglycoside antibiotics on hearing.

Attribution 1 Publication: databreaches.net / OHSU.edu Author:
Article Title: Stolen Oregon Health & Science University hard drive contained babies' protected health information
Article URL: <http://www.databreaches.net/stolen-oregon-health-science-university-hard-drive-contained-babies-protected-health-in/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160211-04	Jackson Health System	FL	2/11/2016	Electronic	Medical/Healthcare	Yes - Published #	24,188

A Jackson Health System employee stands accused of stealing around 24,000 patient records over a period of 5 years. Reid is understood to have inappropriately accessed and viewed patient data including names, dates of birth, addresses, and Social Security numbers.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Rogue Employee Steals 24000 Jackson Health System Patient Records
Article URL: <http://www.hipaajournal.com/rogue-employee-steals-24000-jackson-health-system-patient-records-8308/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160211-03	Capezio	NY	2/10/2016	Electronic	Business	Yes - Unknown #	Unknown

In spite of our security measures, cyber attackers forced their way into our website in October 2015, inserting malware into the software supporting our website. The malware was present until late November, when it was discovered. We immediately removed it and took steps to secure our system.

Attribution 1 Publication: VT AG's office / ME AG's office / MT AG' Author:
Article Title: Capezio
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Capezio%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160211-02	Superior Labels / RubberStamps.Net	IA	2/9/2016	Electronic	Business	Yes - Published #	7,000

Several reports of unusual and/or unauthorized activity after shopping with us were received from our customers in a short period of time. As a result, we have been working in conjunction with law enforcement and a leading cybersecurity firm to investigate these reports. Based on our investigation, it appears that hackers used a security vulnerability in the Wordpress blogging software to gain access to our order management system from November 3, 2015 to December 11, 2015. During that period, the hackers may have been able to access orders placed through our order management system.

Attribution 1 Publication: VT AG's office / CA AG's office / IN AG's Author:
Article Title: Superior Labels
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Superior%20Labels%20-%20Rubberstamps%20SBN%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160211-01	Brightview (formerly Brickman Group, Ltd. LLC)	MD	2/3/2016	Electronic	Business	Yes - Published #	730

On February 3, 2016, an unknown, unauthorized person sent a phishing email requesting that they be provided with specific personal information of our team members (e.g., Social Security number and date of birth). A document that included the personal information of all active team members on our legacy Brickman payroll system was sent to the unknown party in response. This incident was not the result of an intrusion into our computer systems or network. BrightView continues to actively investigate the matter.

Attribution 1 Publication: CA AG's office SC magazine Author:
Article Title: Brightview (formerly Brickman Group, Ltd. LLC)
Article URL: <http://www.scmagazine.com/phishing-scam-nets-pii-from-730-brightview-employees/article/473589/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160210-01	Washington State Health Authority (HCA) / Medicaid	WA	2/10/2016	Electronic	Medical/Healthcare	Yes - Published #	91,187

Both employees assert that the exchange of information occurred because the HCA employee needed technical assistance with spreadsheets that contained the data and that the information was not used for any additional unauthorized purposes or forwarded to any other unauthorized recipients," according to a news release. "The breach was discovered in the course of a whistleblower investigation into misuse of state resources.

Attribution 1 Publication: Q13fox.com Author:
Article Title: State notifies 91,000 Apple Health (Medicaid) clients of data breach
Article URL: <http://q13fox.com/2016/02/09/state-notifies-91000-apple-health-medicaid-clients-of-data-breach/>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 211 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160209-02	Seim Johnson, LLP	NE	2/8/2016	Electronic	Medical/Healthcare	Yes - Published #	30,972

The letter informed patients that a Seim Johnson laptop computer was stolen and that their personal information about services they received at Community Hospital may be affected. Seim Johnson is an accounting firm in Omaha and provides services to Community Hospital. In order to perform these services, Seim Johnson receives limited information about a sample of patients to audit the hospital's financial activities.

Attribution 1 Publication: [hhs.gov / mccookgazette.com](http://hhs.gov/mccookgazette.com) Author:
Article Title: Theft of auditing firm's computer affects local patients
Article URL: <http://www.mccookgazette.com/story/2276069.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160209-01	Department of Homeland Security / FBI	DC	2/8/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

Computer hackers have accessed and dumped personal information of more than 9,000 Department of Homeland Security employees, and the hackers suggest they have the information of more than 20,000 FBI employees, reports Motherboard. Breached information includes names, job titles, email addresses and phone numbers of employees.

Attribution 1 Publication: beckershospitalreview.com Author:
Article Title: Hackers breach 9,000 DHS employees, say FBI is next
Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/hackers-breach-9-000-dhs-employees-say-f>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160208-03	University of Mary Washington	VA	2/4/2016	Electronic	Educational	Yes - Published #	4,100

On January 5, 2016, UMW was informed by a university employee that an issued laptop computer was stolen while in transit. Upon learning this, UMW immediately began an investigation and determined that the laptop stored files containing your name, address, and Social Security number. The employee contacted law enforcement, but to date, law enforcement has been unable to locate the computer.

Attribution 1 Publication: VT AG's office Author:
Article Title: University of Mary Washington
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/University%20of%20Mary%20Washington%20SBN%20

Attribution 2 Publication: databreaches.net / NH AG's office / MT Author:
Article Title: Stolen University of Mary Washington laptop held SSN (UPDATED)
Article URL: <http://www.databreaches.net/va-stolen-university-of-mary-washington-laptop-held-ssn/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160208-02	Baja Bound Insurance Services, Inc.	CA	2/8/2016	Electronic	Business	Yes - Unknown #	Unknown

On December 16, 2015, we discovered that an agent's Baja Bound Insurance Service's email account may have been compromised through a phishing attack. From our investigation, it appears the phishing email was intended to collect only email addresses. As part of our investigation, we also reviewed the documents stored in the email account and discovered an application that contained your personal information, including your name, address, date of birth, and driver's license number.

Attribution 1 Publication: CA AG's office / MT AG's office Author:
Article Title: Baja Bound Insurance Services, Inc.
Article URL: <https://dojmt.gov/wp-content/uploads/Baja-Bound-Insurance-Services.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160208-01	GYFT	CA	2/5/2016	Electronic	Business	Yes - Unknown #	Unknown

Beginning on October 3 and continuing through December 18, 2015, an unknown party accessed without authorization two cloud providers used by Gyft. This unknown party was able to view or download certain Gyft user information stored with these cloud providers and make a file containing some of that user information.

Attribution 1 Publication: CA AG's office / MT AG's office Author:
Article Title: GYFT
Article URL: https://oag.ca.gov/system/files/Multistate%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160205-03	Department of Human Resource Management	VA	1/15/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

Earlier this week, Jigsaw Security noted that they had discovered that improper redaction of documents posted on the Virginia Dept of Human Resource Management website was potentially exposing employees' personal information: A PDF posted by this organization contained information that was obfuscated by blocks but was a layered image so if you edit the document the blocks can be removed and the original content is then visible.

Attribution 1 Publication: databreaches.net Author:
Article Title: Improper redaction exposed Virginia employees' personal info
Article URL: <http://www.databreaches.net/improper-redaction-exposed-virginia-employees-personal-info/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160205-02	Oakmont High School	CA	2/5/2016	Paper Data	Educational	Yes - Published #	356

A guidance counselor at Oakmont High School took the transcripts home with her to work on over the weekend of Jan. 23. They belonged to students in every grade level with last names beginning with P through Ta. The transcripts contained the student's names, birthdays, their parents' names, phone numbers, grades and addresses. No Social Security numbers were listed.

Attribution 1 Publication: databreaches.net / KCRA.com Author:
Article Title: 356 Oakmont High School students' transcripts stolen from counselor's car
Article URL: <http://www.databreaches.net/ca-356-oakmont-high-school-students-transcripts-stolen-from-counselors-car/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160205-01	Borgess Rheumatology	MI	2/5/2016	Paper Data	Medical/Healthcare	Yes - Published #	700

Borgess Rheumatology is reaching out to hundreds of patients who may have been contacted by mistake. According to a statement Newschannel 3 received Friday morning approximately 700 patient letters were mailed to the wrong patients back on December 9, 2015.

Attribution 1 Publication: databreaches.net / wwmt.com / hipaajou Author:
Article Title: 700 Letters sent to wrong patients at Borgess Rheumatology
Article URL: <http://wwmt.com/news/local/700-letters-sent-to-wrong-patients-at-borgess-rheumatology>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160204-05	Clarks Americas, Inc.	MA	1/11/2016	Electronic	Business	Yes - Unknown #	Unknown

Clarks Americas, Inc.
156 Oak Street, Newton Upper Falls, MA 02464
Michael Petrie, Associate General Counsel, 617-796-5240
12/17/15 (discovered 12/22/15)
1/11/2016
Name and SSN

Attribution 1 Publication: ME AG's office Author:
Article Title: Clarks Americas, Inc.
Article URL: http://www.maine.gov/ag/consumer/identity_theft/index.shtml

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 213 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160204-04	Oak Hill Citgo Gas & Convenience	ME	1/14/2016	Electronic	Business	Yes - Unknown #	Unknown

Oak Hill Citgo Gas and Convenience
230 US Rte 1, P.O. Box 606, Scarborough, ME 04074
Lisa Brady, VP, 207-883-4222, oakhillmobil@securespeed.us
Mid-Dec (discovered 12/12/15)
1/14/2016

Name or other personal identifier in combination with financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Attribution 1 Publication: ME AG's office Author:
Article Title: Oak Hill Citgo Gas & Convenience
Article URL: http://www.maine.gov/ag/consumer/identity_theft/index.shtml

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160204-03	Phillip Capital, Inc.	IL	1/12/2016	Electronic	Business	Yes - Unknown #	Unknown

Phillip Capital, Inc., 141 West Jackson Boulevard, Suite 3050, Chicago, IL 60604
Janet Goodridge, CCO, 312-356-9000, compliance@phillipcapital.com
N/A10/23/15 (Discovered 12/3/15)1/12/2016

Name or other personal identifier in combination with SSN, Driver's license number or non-driver ID card number

Attribution 1 Publication: ME AG's office Author:
Article Title: Phillip Capital, Inc.
Article URL: http://www.maine.gov/ag/consumer/identity_theft/index.shtml

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160204-02	University of Central Florida	FL	2/4/2016	Electronic	Educational	Yes - Published #	63,000

An intrusion into the University of Central Florida's computer network has resulted in unauthorized access to certain personal information of some current and former students and employees. To date, the investigation has determined unauthorized access to Social Security numbers — but not credit card information, financial records, medical records or grades — for approximately 63,000 current and former students, staff and faculty members.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: University of Central Florida hack compromises 63,000 Social Security numbers
Article URL: <http://www.databreaches.net/university-of-central-florida-hack-compromisesq-63000-social-security-numbers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160204-01	Medicap Pharmacy	IA	2/4/2016	Electronic	Medical/Healthcare	Yes - Published #	2,300

The hard drive contained personal information. Medicap believed all of the information was encrypted, but said it learned on Dec. 3 that some information did not have encryption. That hard drive had information about customers who filled prescriptions at the pharmacy located at 2804 Beaver Ave. in Des Moines between June 2014 and Nov. 3, 2015, Medicap said. Information included names, addresses, date of birth, telephone numbers, prescriber information, names of medications, costs, insurance information and social security numbers.

Attribution 1 Publication: databreaches.net / desmoinesregister.co Author:
Article Title: Medicap Pharmacy warns of possible data breach
Article URL: <http://www.databreaches.net/ia-medicap-pharmacy-warns-of-possible-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160203-03	Berks & Beyond Employment Services	PA	1/16/2016	Paper Data	Business	Yes - Unknown #	Unknown

She told me she notified the recycling center's yard attendant, who told her the papers had been dumped there earlier in the day, Jan. 6, and the contents of the bin were scheduled to be shredded in a few days. The paperwork was from Berks & Beyond Employment Services, a staffing agency with offices in eastern and central Pennsylvania, including Allentown, Breinigsville and Reading.

Attribution 1 Publication: www.mcall.com Author:
Article Title: Personal information of job applicants exposed in Allentown
Article URL: <http://www.mcall.com/news/local/watchdog/mc-employment-agency-applications-exposed-watchdog-20160116-colum>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160203-02	Crest Foods	OK	1/18/2016	Paper Data	Business	Yes - Unknown #	Unknown

An anonymous tipster sent News 9 five images and claimed they were taken behind Corrugated Services. The images show what looks like Crest Foods employment documents (applications, direct deposit form, etc.) with piles of cardboard in the background.

Attribution 1 Publication: www.news9.com Author:
Article Title: Personal Information Found On Discarded Crest Foods Job Applications
Article URL: <http://www.news9.com/story/30995309/personal-information-found-on-discarded-crest-foods-job-applications>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160203-01	Richardson & Company, P.C.	MA	1/29/2016	Electronic	Business	Yes - Unknown #	Unknown

On December 21, 2015, Richardson discovered that an employee who concluded his employment with the firm on December 18, 2015, had downloaded certain Richardson business records from Richardson's server to an external drive. Some of the documents downloaded from the Richardson server included client social security numbers and financial account numbers, along with customer names and addresses.

Attribution 1 Publication: NH AG's office / ME AG's office / MT AG Author:
Article Title: Richardson & Company, P.C.
Article URL: <http://doj.nh.gov/consumer/security-breaches/documents/richardson-20160129.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160202-03	Crown Point Health Center	IN	1/29/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,854

"Patients' empty paper file folders with protected health information (PHI) appearing on the front cover were improperly disposed of when an employee put them in the regular trash. The PHI on the cover included patients' dates of birth, medical record numbers, and guarantors' names. Approximately 1,854 individuals were affected by this breach. The covered entity (CE) provided breach notification to HHS, affected individuals and the media. The notification letter informed the individuals that a hotline had been established to address their questions and provided the hotline phone number. To prevent a similar breach from happening in the future, the CE sanctioned the involved employee and counseled the remaining staff regarding this matter. OCR obtained assurances that the CE implemented the corrective actions listed above."

Attribution 1 Publication: hhs.gov Author:
Article Title: Crown Point Health Center
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160202-02	Hawaii Medical Service Association	HI	1/15/2016	Paper Data	Medical/Healthcare	Yes - Published #	10,179

The Hawai'i Medical Service Association (HMSA) is notifying about 10,800 members that it mistakenly sent care management letters to incorrect addresses. The misrouted letters did NOT contain financial information, Social Security numbers, HMSA membership numbers, birth dates, claims information, or medical histories. The letters did include member names and steps they could take to identify and manage certain health conditions, such as asthma, diabetes, and lung and heart disease.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Hawai'i Medical Service Association Privacy Breach Affects 10,800
Article URL: <http://www.hipaajournal.com/hawaii-medical-service-association-privacy-breach-8293/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160202-01	International Alliance of Theatrical Stage Employees	CA	1/21/2016	Electronic	Business	Yes - Unknown #	Unknown

We are writing to you because we have been informed a laptop belonging to IA 134 and connected to the network at Levi's Stadium was breached via the internet on January 4th and information was taken from the computer. An investigation is under way but we do not know what information may have been compromised. It is possible that your name and Social Security number have been taken.

Attribution 1 Publication: CA AG's office Author:
Article Title: International Alliance of Theatrical Stage Employees #134
Article URL: https://oag.ca.gov/system/files/IA%20134%20info%20notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-14	Shannon Tax & Business Services	NM	1/27/2016	Paper Data	Business	Yes - Unknown #	Unknown

It's tax season, and that means a lot of sensitive information is getting printed on a lot of pieces of paper. Action 7 News found some of that paper just lying in an Albuquerque dumpster. That stuff is a stack of documents containing people's personal information, including social security numbers. They were seen in a dumpster outside an Albuquerque tax preparation business by an Action 7 News viewer.

Attribution 1 Publication: databreaches.net / KOAT.com Author:
Article Title: Documents with Social Security numbers found in Albuquerque dumpster
Article URL: <http://www.koat.com/news/documents-with-social-security-numbers-found-in-albuquerque-dumpster/37656832>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-13	cPanel	TX	1/27/2016	Electronic	Business	Yes - Unknown #	Unknown

I am writing to let you know that one of our user databases may have been breached. Although we successfully interrupted the breach, it is still possible that user contact information may have been susceptible. The customer contact information that may have been susceptible is limited to names, contact information, and encrypted (and salted) passwords. Please note that our credit card information is stored in a separate system designed for credit card storage and is not impacted by this possible breach.

Attribution 1 Publication: databreaches.net Author:
Article Title: Important Information for cPanel Store Users
Article URL: <http://www.databreaches.net/important-information-for-cpanel-store-users/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-12	Florida International University	FL	1/28/2016	Electronic	Educational	Yes - Unknown #	Unknown

On January 16, DataBreaches.net attempted to notify Florida International University about a possible hack after seeing email addresses and plain text passwords of what appear to be faculty and students at FIU have been dumped on a paste site. This site sent FIU a sample of the records in the paste with a link to the paste, noting that there were about 160 addresses with passwords in one section of the data dump, and that another section included first and last names, usernames, encrypted passwords, and email addresses.

Attribution 1 Publication: databreaches.net Author:
Article Title: Florida International University data hacked and dumped: claim
Article URL: <http://www.databreaches.net/florida-international-university-data-hacked-and-dumped-claim/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-11	Louisiana Healthcare Connections	LA	1/30/2016	Electronic	Medical/Healthcare	Yes - Published #	13,086

Robinson was charged with one count of identity theft, one count of computer fraud, and one count of criminal conspiracy to commit Medicaid fraud after downloading over 13,000 Medicaid Recipient's information from Louisiana Healthcare Connections, a Louisiana Managed Care Organization.

Attribution 1 Publication: databreaches.net / hipaajournal.com Author:
Article Title: Medicaid fraud case had 13k victims
Article URL: <http://www.databreaches.net/la-medicaid-fraud-case-had-13k-victims/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-10	Wayne Memorial Hospital	PA	2/1/2016	Electronic	Medical/Healthcare	Yes - Published #	390

A security breach at the Wayne Memorial Hospital in Honesdale causing concerns. Hospital officials tell Eyewitness News they have fired a nurses's aide who they say accessed patient records without authorization.

Attribution 1 Publication: databreaches.net / Pahomepage.com Author:
Article Title: Wayne Memorial Hospital
Article URL: <http://www.pahomepage.com/news/wayne-memorial-hospital-security-breach-concerns>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-09	AHRC Nassau	NY	1/6/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,200

AHRC Nassau NY Healthcare Provider 1200 01/06/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: AHRC Nassau
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-08	G & S Medical Associates, LLC	NJ	1/14/2016	Electronic	Medical/Healthcare	Yes - Published #	3,000

G&S Medical Associates, LLC NJ Healthcare Provider 3000 01/14/2016 Hacking/IT Incident Desktop Computer

Attribution 1 Publication: hhs.gov Author:
Article Title: G & S Medical Associates, LLC
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-07	Livongo Health, Inc.	IL	1/25/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,950

The covered entity (CE) learned that its business associate (BA) mislabeled certain packages containing lancet devices so that the devices were sent and delivered to the correct address, but the shipping label stated the wrong name for the CE's members. The label included the wrong member's name and information from which it could be incorrectly inferred that the individual was to receive a lancet device from the CE and had diabetes. This breach affected 1,950 individuals. The CE provided breach notice to HHS and affected individuals.

Attribution 1 Publication: hhs.gov / MT AG's office Author:
Article Title: Livongo Health, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-06	NCH Healthcare System	FL	1/28/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

An NCH Healthcare System cyberattack has been announced this week which involved two computer servers potentially being accessed by an unauthorized individual.

Attribution 1 Publication: hipaajournal.com / databreaches.net / M Author:
Article Title: NCH Healthcare System Cyberattack Announced
Article URL: <http://www.hipaajournal.com/nch-healthcare-system-cyberattack-8286/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-05	Wendy's	OH	1/27/2016	Electronic	Business	Yes - Unknown #	Unknown

Wendy's, the nationwide chain of fast-food restaurants, says it is investigating claims of a possible credit card breach at some locations. The acknowledgment comes in response to questions from KrebsOnSecurity about banking industry sources who discovered a pattern of fraud on cards that were all recently used at various Wendy's locations.

Attribution 1 Publication: krebsonsecurity.com / SC AG's office Author:
Article Title: 1,025 Wendy's Locations Hit in Card Breach
Article URL: <http://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/>

Attribution 2 Publication: krebsonsecurity.com Author:
Article Title: Wendy's Probes Reports of Credit Card Breach
Article URL: <http://krebsonsecurity.com/2016/01/wendys-probes-reports-of-credit-card-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-04	Alba Botanica	NY	1/28/2016	Electronic	Business	Yes - Unknown #	Unknown

On December 9, 2015, we discovered evidence of a potential vulnerability on the check-out page of www.albaboranica.com. Upon discovering this evidence, we quickly began to investigate this issue and disabled the website to prevent any possible exploitation of the vulnerability. Third-party cyber security experts were retained to assist with the investigation. On December 29, 2015, we discovered that malicious code had been inserted into the check-out page on www.albaboranica.com, and that this code may have resulted in the potential unauthorized access to, or acquisition of, customer payment information entered during the online check-out process at www.albaboranica.com

Attribution 1 Publication: VT AG's office / MT AG's office Author:
Article Title: Alba Botanica
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Hain%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-03	LifeSafer	OH	1/26/2016	Electronic	Business	Yes - Unknown #	Unknown

We are writing today to inform you that LifeSafer, like many other companies, has been the victim of an unauthorized access to our electronic data. Between late December 2015 and early January 2016, an unauthorized party used compromised account credentials on a LifeSafer external website to access personal information. Based upon our investigation, we have determined that this unauthorized access included your personal information, specifically, your name and driver's license number

Attribution 1 Publication: VT AG's office Author:
Article Title: LifeSafer
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/LifeSafer%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-02	TaxSlayer	GA	1/16/2016	Paper Data	Business	Yes - Published #	8,800

As a result of ongoing security reviews, TaxSlayer identified on January 13, 2016 that an unauthorized third party, whom we believe obtained your username and password from another online service, may have accessed your TaxSlayer account between 10/10/2015 and 12/21/2015. We have no evidence indicating that the technical security of TaxSlayer systems has been compromised. What Information Was Involved? The unauthorized third party may have obtained access to any information you included in a tax return or draft tax return saved on TaxSlayer, including your name and address, your Social Security number, the Social Security numbers of your dependents, and other data contained on your 2014 tax return.

Attribution 1 Publication: scmagazine.com Author:
Article Title: TaxSlayer breached: 8,800 customers notified PII may be compromised
Article URL: <http://www.scmagazine.com/taxslayer-breached-8800-customers-notified-pii-may-be-compromised/article/470259/>

Attribution 2 Publication: CA AG's office Author:
Article Title: TaxSlayer
Article URL: https://oag.ca.gov/system/files/TaxSlayer%20CA_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160201-01	Neiman Marcus Group	TX	1/29/2016	Electronic	Business	Yes - Published #	5,200

We are writing to share with you important information about an incident involving your online account username and password, as well as the steps we are taking in response to this incident, recommended actions for you to take, and the resources we are making available to you.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Unauthorized access leads to Neiman Marcus Group breach, 5,200 affected
Article URL: <http://www.scmagazine.com/attacker-accesses-5200-neiman-marcus-group-customer-accounts/article/470237/>

Attribution 2 Publication: CA AG's office Author:
Article Title: Neiman Marcus Group
Article URL: https://oag.ca.gov/system/files/Neiman%20Marcus%20notice%20only%201-29-2016_0_0.pdf?

Attribution 3 Publication: Bankinfosecurity.com Author: Tracy Kitten
Article Title: Neiman Marcus Reports New Breach
Article URL: http://www.bankinfosecurity.com/neiman-marcus-reports-new-breach-a-8843?rf=2016-02-04-eb&mkt_tok=3RkMMJWW

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160126-09	Vermont State Employees	VT	1/23/2016	Electronic	Government/Military	Yes - Unknown #	Unknown

At least 500 state workers fell prey to a phishing scam on Thursday, and state officials say the tax records of as many as 50 employees were compromised. An email with the subject line "IMPORTANT TAX RETURN DOCUMENT AVAILABLE" took unsuspecting state workers to a dummy login landing page that replicated the Department of Human Resources website. The email encouraged employees to click on a link to get access to W-2 information.

Attribution 1 Publication: databreaches.net / vtdigger.com Author:
Article Title: Vermont State Employees
Article URL: <http://vtdigger.org/2016/01/23/state-workers-w-2-info-compromised-in-phishing-scam/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160126-08	Lawrence Public Schools	MA	1/24/2016	Electronic	Educational	Yes - Unknown #	Unknown

Hackers breached Lawrence Public Schools' online database, acquiring teachers' personal information, possibly including their Social Security numbers, school officials said. In the email, Riley said the breach may have disclosed employees' names, phone numbers, addresses, Social Security numbers and calendar year 2015 gross earnings. However, the breach did not include any employees' bank account information, according to Rile

Attribution 1 Publication: databreaches.net / eagletribune.com Author:
Article Title: Teachers' personal data hacked
Article URL: http://www.eagletribune.com/news/teachers-personal-data-hacked/article_47d05336-ad23-568b-a36a-ae2b2cdf7284.ht

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160126-07	Hudson City School District	NY	1/24/2016	Electronic	Educational	Yes - Unknown #	Unknown

The Hudson City School District was the victim of a phishing scam when two emails posing as the district's superintendent came through the email system.

"As a result, employee information of all district staff including individual social security numbers were fraudulently obtained by an unauthorized individual," the email read.

Attribution 1 Publication: databreaches.net / thedailyemail.com Author:
Article Title: Hudson City School District employees hit by phishing scheme
Article URL: http://www.thedailyemail.net/news/article_cff84f8c-c261-11e5-98b1-4f5635367d1f.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160126-06	Centene	MO	1/26/2016	Electronic	Medical/Healthcare	Yes - Published #	950,000

Centene, a St. Louis-based payer, is searching for six missing hard drives that contain protected health information of approximately 950,000 individuals. The six hard drives contain information of individuals who received laboratory services from 2009 to 2015, including names, addresses, birth dates, Social Security numbers, member ID number and health information. There is no financial or payment information stored on the hard drives, according to the payer.

Attribution 1 Publication: savannahnow.com Author: Andy Miller
Article Title: Data breach affects thousands in Georgia Medicaid, PeachCare
Article URL: <http://savannahnow.com/news/2016-02-03/data-breach-affects-thousands-georgia-medicaid-peachcare>

Attribution 2 Publication: beckershospitalreview.com Author:
Article Title: Centene missing hard drives with 950,000 members' information
Article URL: <http://www.beckershospitalreview.com/healthcare-information-technology/centene-missing-hard-drives-with-950-000->

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160126-05	Baileys, Inc.	CA	1/11/2016	Electronic	Business	Yes - Published #	250,000

Recently, an examination by our computer security consultant revealed that someone without authorization accessed and likely stole credit card information belonging to our customers from our website. The theft involved @15,000 credit cards used to pay for purchases on our website during the above time frame. Of these @15,000 cards, nearly 25% were MasterCard® cards, 64% were VISA® cards, and fewer than 5% and 6% were American Express® and Discover® cards, respectively.

Attribution 1 Publication: CA AG's office Author:
Article Title: Baileys, Inc.
Article URL: https://oag.ca.gov/system/files/CC%201%20CA%20Notice%20of%20Data%20Breach_0.pdf?

Attribution 2 Publication: Scmagazine.com Author:
Article Title: Attacker compromises information of 250K in Bailey's data breach
Article URL: <http://www.scmagazine.com/attacker-compromises-information-of-250k-in-baileys-data-breach/article/483630/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160126-04	HealthEquity	UT	1/25/2016	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On December 14, 2015, we discovered that a HealthEquity employee inadvertently sent an email on December 11 containing some of your personal information to another employer with whom HealthEquity does business with. We took immediate actions to correct it, including confirming that the recipients had deleted the e-mail.

Attribution 1 Publication: CA AG's office Author:
Article Title: HealthEquity
Article URL: https://oag.ca.gov/system/files/HealthEquity%20CA%20Notification%20inc1142_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160126-03	RealSelf, Inc.	WA	1/25/2016	Electronic	Business	Yes - Unknown #	Unknown

For a brief period over the holiday weekend, an unauthorized party gained access to some consumer data from our servers. We are taking this very seriously and apologize for any inconvenience this may cause during the holiday season. As part of this incident, it is possible that personal information may have been compromised. Here's what you should know: • This information may include your username, email address and a securely hashed version of your password. We never store passwords in plain text. • It DID NOT INCLUDE credit card data or any other personal banking information, which we do not store.

Attribution 1 Publication: CA AG's office Author:
Article Title: RealSelf, Inc.
Article URL: https://oag.ca.gov/system/files/RealSelf%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160126-02	Kicky Pants, Inc.	CA	1/21/2016	Electronic	Business	Yes - Unknown #	Unknown

On December 31, 2015, Kicky Pants, Inc., d/b/a KicKee Pants, discovered evidence of a data security breach that allowed some confidential customer information to be acquired by an unknown third party. What Information Was Involved: The compromised information included first and last names; credit card number, expiration date, and security code; billing address (street, city, state, and ZIP code); telephone number; and email address.

Attribution 1 Publication: CA AG's office / ME AG's office Author:
Article Title: Kicky Pants, Inc.
Article URL: https://oag.ca.gov/system/files/KickyPants%20General%20Notice_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 220 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160122-02	University of Virginia	VA	1/22/2016	Electronic	Educational	Yes - Published #	1,400

In collaboration with the FBI, the University confirmed that, as a result of a “phishing” email scam, unauthorized individuals illegally accessed a component of our human resources system, exposing personally identifiable information of a subset of Academic Division employees. The exposure does not include UVA Medical Center information as it is on a separate system.

Attribution 1 Publication: scmagazine.com Author:
Article Title: University of Virginia hit with Phishing scam, 1,400 affected
Article URL: <http://www.scmagazine.com/university-of-virginia-hit-with-phishing-scam-1400-affected/article/467224/>

Attribution 2 Publication: nbc29.com Author:
Article Title: FBI Alerts UVA to Employee Information Data Breach
Article URL: <http://www.nbc29.com/story/31033287/fbi-alerts-uva-to-employee-information-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160122-01	Blue Dolphin	CT	1/20/2016	Electronic	Business	Yes - Unknown #	Unknown

On December 7, 2015, Blue Dolphin learned that an unauthorized individual gained access to a database containing our customer records. We immediately engaged independent IT forensic experts to assist with our investigation. While the investigation is ongoing, it appears that the individual was able to access the information in the file, which included your name, address, credit or debit card number, and the card's expiration date.

Attribution 1 Publication: VT AG's office / ME AG's office Author:
Article Title: Blue Dolphin
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Blue%20Dolphin%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160121-02	Elite Imaging	FL	1/4/2016	Paper Data	Medical/Healthcare	Yes - Published #	1,457

A log book (sign-in book) containing information about the covered entity's (CE) patients was stolen from its offices and returned anonymously with a letter. The log-book contained the patients' full names and the name of the procedure conducted for each patient. The breach affected 1,457 patients. The CE provided breach notification to HHS, affected individuals, and the media. The CE conducted a full review of the incident and filed a police report. It also reviewed and modified its safeguards policies and internal procedures, implemented a new log in procedure, updated its software, and re-trained all staff received on its new policies. The CE's shredding vendor securely disposed of the log books. OCR obtained assurances that the CE implemented the corrective actions listed above.

Attribution 1 Publication: hhs.gov Author:
Article Title: Elite Imaging
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160121-01	County of San Diego	CA	1/21/2016	Electronic	Government/Military	Yes - Published #	620

The County of San Diego's Benefits Division became aware of an issue involving Wells Fargo Health Savings Accounts (HSA) on December 17, 2015. Data regarding County employees who elected to set up HSAs was sent to Wells Fargo. In addition, however, to the information of the employees who elected this benefit option, your information was inadvertently sent to Wells Fargo as well.

Attribution 1 Publication: scmagazine.com Author:
Article Title: San Diego County employees data mistakenly sent to Wells Fargo
Article URL: <http://www.scmagazine.com/san-diego-county-employees-data-mistakenly-sent-to-wells-fargo/article/466905/>

Attribution 2 Publication: CA AG's office Author:
Article Title: County of San Diego
Article URL: https://oag.ca.gov/system/files/cosd_12_17_2015_0.pdf?

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 221 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160120-07	Fitchburg State University	ME	1/20/2016	Electronic	Educational	Yes - Published #	393

A student notified the school that they were able to see and download an Excel spreadsheet that contained PII while they were searching Google Drive on the student domain. (Reported to MA Office of Consumer Affairs 4/10/2015)

Attribution 1 Publication: metrowestdailynews.com Author:
 Article Title: Fitchburg State University
 Article URL: <http://www.metrowestdailynews.com/massdatabreaches?refresh=true>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160120-06	Town of Amherst	MA	1/20/2016	Electronic	Government/Military	Yes - Published #	414

The Town of Amherst became aware that certain personal information located on its website related to the online payment of utilities in Town was, under certain circumstances, publicly available. This information included residents' financial account numbers if certain searching criteria was used online. (Late reporting by MA Office of Consumer Affairs)

Attribution 1 Publication: metrowestdailynews.com Author:
 Article Title: Town of Amherst
 Article URL: <http://www.metrowestdailynews.com/massdatabreaches?refresh=true>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160120-05	Bevo POS	FL	1/20/2016	Electronic	Business	Yes - Published #	799

American Express is reporting a breach of security of a merchant, the merchant information is as follows. Bevo POS, 6201 Lee Ann Lane, Naples FL 34109. The Merchants POS was hacked and subsequently loaded malware impacting merchant base of POS. (Late reporting by MA Office of Consumer Affairs)

Attribution 1 Publication: krebsonsecurity.com Author:
 Article Title: POS Providers Feel Brunt of PoSeidon Malware
 Article URL: <http://krebsonsecurity.com/2015/04/pos-providers-feel-brunt-of-poseidon-malware/-more-30585>

Attribution 2 Publication: metrowestdailynews.com Author:
 Article Title: Bevo POS
 Article URL: <http://www.metrowestdailynews.com/massdatabreaches?refresh=true>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160120-04	Anna Maria College	ME	1/20/2016	Paper Data	Educational	Yes - Published #	1,161

An employee intended to send an email to a student with the student's financial statement, but because of a software error the attachment actually contained the 1098T forms of 1590 students at the college. (Late reporting by MA Office of Consumer Affairs)

Attribution 1 Publication: metrowestdailynews.com Author:
 Article Title: Anna Maria College
 Article URL: <http://www.metrowestdailynews.com/massdatabreaches?refresh=true>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160120-03	Mrs. Fields Gifts	CO	1/20/2016	Electronic	Business	Yes - Published #	1,769

American Express is notifying us of a breach of a US merchant. The merchant information is as follows: Mrs. Fields Gifts, 2855 E. Cottonwood Pkwy, Salt Lake, UT 84121. The attacker placed malware in the form of a malicious webshell on the compromised system merchant website to gain unauthorized access to cardholder data. On January 7, 2013, a second malicious webshell was installed on the merchant website along with a malicious data aggregation script. (Late reporting by MA Office of Consumer Affairs)

Attribution 1 Publication: metrowestdailynews.com Author:
 Article Title: Mrs. Fields Gifts
 Article URL: <http://www.metrowestdailynews.com/massdatabreaches?refresh=true>

How is this report produced? What are the rules? See last page of report for details.

Report Date: 1/18/2017

Page 222 of 226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160120-02	Rockland Trust	MA	1/20/2016	Electronic	Banking/Credit/Financial	Yes - Published #	2,182

Three individuals had attached, and then removed "skimming" devices and miniature cameras to ATMs and or ATM vestibule door card readers . The skimming devices and cameras were used to obtain names, pin numbers and ATM/debit card numbers of individuals who had used the ATM. The fraudulent transactions originated in New York. (Late reporting by MA Office of Consumer Affairs)

Attribution 1 Publication: metrowestdailynews.com Author:
Article Title: Rockland Trust
Article URL: <http://www.metrowestdailynews.com/massdatabreaches?refresh=true>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160120-01	Credit Union of the Berkshires	MA	1/20/2016	Electronic	Banking/Credit/Financial	Yes - Published #	2,200

They were notified of a data security incident/breach involving their website. The website was defaced by the use of malicious script which was inserted into the coding of the website. (Late reporting by MA Office of Consumer Affairs)

Attribution 1 Publication: metrowestdailynews.com Author:
Article Title: Credit Union of the Berkshires
Article URL: <http://www.metrowestdailynews.com/massdatabreaches?refresh=true>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160119-09	WhiteGlove Health	TX	1/19/2016	Electronic	Medical/Healthcare	Yes - Published #	975

WhiteGlove Health TX Healthcare Provider 975 12/23/2015 Unauthorized Access/Disclosure Email. Late 2015 entry by hhs.gov

Attribution 1 Publication: hhs.gov Author:
Article Title: WhiteGlove Health
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160119-08	Allina Health	MN	1/19/2016	Paper Data	Medical/Healthcare	Yes - Published #	6,195

Allina Health MN Healthcare Provider 6195 12/23/2015 Improper Disposal Paper/Films. Late 2015 entry by hhs.gov

Attribution 1 Publication: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf Author:
Article Title: Allina Health
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160119-07	Brigham and Women's Hospital	MA	1/11/2016	Electronic	Medical/Healthcare	Yes - Published #	1,009

On November 13, 2015, Brigham learned that an unauthorized party obtained the network credentials of one of our employees and used those credentials to access that employee's email account. Through comprehensive review of the affected email account, we determined that the emails potentially contained information for a limited number of individuals including full name, date of birth, medical record number, provider name, date of service, and some clinical information, such as diagnosis and treatment received.

Attribution 1 Publication: [hhs.gov / databreaches.net](http://hhs.gov/databreaches.net) / MA AG's of Author:
Article Title: Brigham and Women's Hospital
Article URL: <http://www.databreaches.net/compromised-email-account-exposed-patient-info-from-brigham-and-womens-and-brigh>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160119-06	New West Health Services	MT	1/15/2016	Electronic	Medical/Healthcare	Yes - Published #	28,209

On November 18, 2015, a New West Health Services laptop computer was stolen from an off-site location when an employee was out of the office traveling on business. The computer contained electronic files with personal information from past and present New West customers.

Attribution 1 Publication: [esecurityplanet.com / hhs.gov / NH AG's](http://esecurityplanet.com/hhs.gov/NH-AGs) Author:
 Article Title: Medical Data Breaches at Blue Shield, New West Expose 46,000 Customers' Info
 Article URL: <http://www.esecurityplanet.com/network-security/medical-data-breaches-at-blue-shield-new-west-affect-46000-custom>

Attribution 2 Publication: VT AG's office Author:
 Article Title: New West Health Services
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/New%20West%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160119-05	TaxAct / Blucora, Inc.	IA	1/12/2016	Electronic	Business	Yes - Published #	450

We have concluded that an unauthorized third party accessed your TaxAct account between November 10 and December 4, 2015. We have no evidence that any TaxAct system has been compromised and believe the third party used username and password combinations obtained from sources outside of our own system. In order to stop this unauthorized access, we have temporarily disabled your account.

Attribution 1 Publication: accountingtoday.com Author:
 Article Title: TaxAct Detects Data Breach and Suspends Customer Accounts
 Article URL: <http://www.accountingtoday.com/news/tax-practice/taxact-detects-data-breach-and-suspends-customer-accounts-769>

Attribution 2 Publication: CA AG's office / VT AG's office / esecuri Author:
 Article Title: TaxAct Acknowledges Data Breach
 Article URL: <http://www.esecurityplanet.com/network-security/taxact-acknowledges-data-breach.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160119-04	JB Autosports	IA	1/19/2016	Electronic	Business	Yes - Published #	1,000

From approximately August 1, 2015 through November 9, 2015, the websites' checkout page where customers input their payment information to purchase products from JB Autosports was the target of a cyberattack originating from a Russian IP address. The breach affected customers who used Visa, MasterCard, Discover, and American Express branded cards to pay for their purchases from the websites.

Attribution 1 Publication: CA AG's office / VT AG's office / ME AG' Author:
 Article Title: JB Autosports
 Article URL: https://oag.ca.gov/system/files/00631462_0.PDF?

Attribution 2 Publication: CSOnline Author:
 Article Title: JB Autosports Inc. - Checkout system compromised
 Article URL: [CSO Online's 2016 data breach blotter](http://www.csosonline.com/2016/01/19/jb-autosports-checkout-system-compromised/)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160119-03	RateMyProfessors.com	NY	1/12/2016	Electronic	Business	Yes - Unknown #	Unknown

On December 24, 2015, RateMyProfessors.com first noticed anomalous activity associated with one of the backend systems used by RateMyProfessors.com. RateMyProfessors.com investigated and subsequently learned that, on or about November 26, 2015, hackers gained access to a decommissioned version of the RateMyProfessors.com website ("Decommissioned Site") by exploiting a vulnerability in an Internet facing application within the Decommissioned Site.

Attribution 1 Publication: CA AG's office Author:
 Article Title: RateMyProfessors.com
 Article URL: <https://oag.ca.gov/system/files/RateMyProfessors%20User%20Notification%2020160106%20-%20Attach%20to%20Calif>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160119-02	HSBC Bank USA, N.A.	NY	1/13/2016	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently became aware of an incident in which HSBC's mortgage servicing provider sent encrypted and password protected disks, which inadvertently included some of your personal information, to an unauthorized commercial third party (a firm that performs financial analytics).

Attribution 1 Publication: CA AG's office / VT AG's office / SC AG' Author:
 Article Title: HSBC Bank USA, N.A.
 Article URL: https://oag.ca.gov/system/files/IdGrd_1_Version6%20Public_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160119-01	Blue Shield of California	CA	1/14/2016	Electronic	Medical/Healthcare	Yes - Published #	20,764

In December of 2015, Blue Shield was notified by our vendor that data about you may have been accessed by an unauthorized user who gained access to the vendor's data systems without permission.

Attribution 1 Publication: esecurityplanet.com Author:
 Article Title: Medical Data Breaches at Blue Shield, New West Expose 46,000 Customers' Info
 Article URL: <http://www.esecurityplanet.com/network-security/medical-data-breaches-at-blue-shield-new-west-affect-46000-custom>

Attribution 2 Publication: CA AG's office / hhs.gov Author:
 Article Title: Blue Shield of California
 Article URL: https://oag.ca.gov/system/files/Member%20Adult_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160112-02	Oceans Acquisition, Inc.	TX	1/12/2016	Electronic	Medical/Healthcare	Yes - Published #	659

The potential exposure occurred when a laptop was stolen from an employee's car. The laptop stored emails that potentially contained PHI such as names, dates of birth, medical record numbers, diagnoses, payer information and admission dates. No patient social security numbers or bank account information was included in the emails.

Attribution 1 Publication: txheadlines.com / databreaches.net Author:
 Article Title: Oceans Acquisition, Inc.
 Article URL: http://www.txheadlines.com/index.php/public_notices/article/Notification-of-Potential-Data-Breach-In-December-2015-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160112-01	St. Luke's Cornwall Hospital	NY	1/12/2016	Electronic	Medical/Healthcare	Yes - Published #	29,156

On October 31, 2015, an individual entered a restricted area of St. Luke's Cornwall Hospital ("SLCH") and stole a USB thumb drive that may have contained limited protected health information for some patients. SLCH takes the privacy and security of its patients' information very seriously and is cooperating with law enforcement personnel in their investigation. Late 2015 entry by hhs.gov

Attribution 1 Publication: databreaches.net / hhs.gov Author:
 Article Title: St. Luke's Cornwall Hospital notifies patients after thumb drive with limited PHI is stolen
 Article URL: <http://www.databreaches.net/ny-st-lukes-cornwall-hospital-notifies-patients-after-thumb-drive-with-limited-phi-is-stole>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160111-01	Pittman Family Dental	OH	1/11/2016	Electronic	Medical/Healthcare	Yes - Published #	8,830

Pittman Family Dental OH Healthcare Provider 8830 12/31/2015 Hacking/IT Incident Network Server. Late 2015 entry by HHS.gov

Attribution 1 Publication: hhs.gov Author:
 Article Title: Pittman Family Dental
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160108-04	Time Warner Cable	TX	1/8/2016	Electronic	Business	Yes - Unknown #	Unknown

Up to 320,000 Time Warner Cable customers may have had their email passwords stolen resulting from a variety of hacking methods, company officials confirmed this week. The Reuters news service reported the customers' data may have been compromised through malware downloaded during phishing attacks or indirectly through other types of data breaches.

Attribution 1 Publication: patch.com Author:
Article Title: Time Warner Cable Confirms Major Data Breach
Article URL: <http://patch.com/texas/downtownaustin/time-warner-cable-confirms-major-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160108-03	Fidelis Care	NY	1/7/2016	Paper Data	Medical/Healthcare	Yes - Published #	738

Fidelis Care NY Health Plan 738 12/15/2015 Unauthorized Access/Disclosure Paper/Films. Late 2015 entry by HHS.gov

Attribution 1 Publication: hhs.gov Author:
Article Title: Fidelis Care
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160108-01	Indiana University Health Arnett Hospital	IN	1/8/2016	Electronic	Medical/Healthcare	Yes - Published #	29,324

On November 20, 2015, we learned that an unencrypted portable storage device was missing from the Emergency Department, and an ongoing search continues. We immediately began an investigation and determined that the device contained spreadsheets with limited patient information from Emergency Department visits that occurred between November 1, 2014 and November 20, 2015. The spreadsheets may have included patients' names, dates of birth, ages, home telephone numbers, medical record numbers, dates of service, diagnoses and treating physicians.

Attribution 1 Publication: databreaches.net Author:
Article Title: IU Health Arnett Hospital notified 30,000 of missing or stolen portable storage device
Article URL: <http://www.databreaches.net/iu-health-arnett-hospital-notified-30000-of-missing-or-stolen-portable-storage-device/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160106-01	Southern New Hampshire University	NH	1/5/2016	Electronic	Educational	Yes - Published #	140,000

Southern New Hampshire University (SNHU) says they're still investigating how a database containing some student and class information was exposed to the public. The database was discovered by researcher Chris Vickery shortly before Christmas. The exposed SNHU database contains more than 140,000 records including student names, email addresses, and IDs; as well as other class-related details such as course name, course section, assignment details and assignment score. The database also contains instructor names and email addresses.

Attribution 1 Publication: csoonline.com / databreaches.net Author:
Article Title: SNHU still investigating database leak exposing over 140,000 records
Article URL: <http://www.csoonline.com/article/3019278/security/snhu-still-investigating-database-leak-exposing-over-140-000-recor>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20160105-01	Regional Income Tax Authority	OH	1/4/2016	Electronic	Business	Yes - Published #	50,000

The Regional Income Tax Agency announced Dec. 31 that nearly two months earlier it lost personal data for about 50,000 people who filed tax forms with the agency. The agency Nov. 10 discovered it could not find a DVD that contained copies of income tax documents submitted on or before June 2012. The DVD may have contained names, addresses, Social Security numbers and dates of birth. Arrighi said the agency waited to announce the missing information until its investigation was complete.

Attribution 1 Publication: cleveland.com/metro / VT AG's office Author:
Article Title: RITA loses personal info for 50,000 people, offers free credit monitoring
Article URL: http://www.cleveland.com/metro/index.ssf/2016/01/rita_loses_personal_info_for_5.html

2016 Breaches Identified by the ITRC as of: 1/18/2017

Total Breaches: 1,093
Records Exposed: 36,601,939

The ITRC Breach database is updated on a daily basis, and published to our website on Tuesday. Unless noted otherwise, each report includes breaches that occurred in the year of the report name (such as "2016 Breach List"), or became public in the report name year, but were not public in the previous year. Each item must be previously published by a credible source, such as an Attorney General's website, network television, national print media, etc. The item will not be included if the ITRC is not certain that the source is real and credible. We include, for each incident, a link or source of the article, and the information presented by that article. Many times, we have attributions from a multitude of media sources and media outlets. ITRC sticks to the facts as reported, and does not add or subtract from the previously published information. When the number of exposed records is not reported, we note that fact. Note: For data breach incidents involving only emails, user names, and/or passwords, the number of records are not included in the overall total number of records.

What is a breach? A breach is defined as an event in which an individual's name plus Social Security Number (SSN), driver's license number, medical record, or a financial record/credit/debit card is potentially put at risk – either in electronic or paper format.

The ITRC Breach Report presents individual information about data exposure events and running totals for the year.

The ITRC Breach Stats Report develops some statistics based upon the type of entity involved in the data exposure.



The ITRC would like to thank CyberScout for its financial support of the ITRC Breach Report, ITRC Breach Stats Report and all supplemental breach reports.