



DATA BREACH REPORTS

June 30, 2018



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

CONTENTS

Information & Background on ITRC	3
Methodology	4
ITRC Breach Stats Report Summary	5
ITRC Breach Stats Report	6
ITRC Breach Report	33

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 in the cumulative annual total.

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 (which includes Spearphishing, Ransomware, and Skimming), Data on the Move, Employee error/Negligence/Improper disposal/Lost, Accidental web/Internet Exposure, Physical Theft and Unauthorized Access. (Please note that Accidental email, previously included with Accidental web/Internet Exposure, has been re-categorized under the Employee error/Negligence/Improper disposal/Lost category.) Subcontractor/Third Party/BA is included here but is combined with one of the above. In these, as well as some other breaches, there may be more than one category checked.

The ITRC breach list also tracks types of information compromised:

- Social Security number
- Credit/Debit Card number
- Protected Health Information (PHI)
- DMV Records
- Financial Accounts
- Email/Password/User Name
- 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

2018 - Data Breach Category Summary

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

Report Date: 7/2/2018

Totals for Category: Banking/Credit/Financial	# of Breaches: 84 % of Breaches: 12.6	# of Records: 1,705,354 %of Records: 7.6%
Totals for Category: Business	# of Breaches: 309 % of Breaches: 46.3	# of Records: 15,213,588 %of Records: 67.9%
Totals for Category: Educational	# of Breaches: 45 % of Breaches: 6.7%	# of Records: 642,270 %of Records: 2.9%
Totals for Category: Government/Military	# of Breaches: 49 % of Breaches: 7.3%	# of Records: 1,598,501 %of Records: 7.1%
Totals for Category: Medical/Healthcare	# of Breaches: 181 % of Breaches: 27.1	# of Records: 3,248,545 %of Records: 14.5%
Totals for All Categories:	# of Breaches: 668 % of Breaches: 100.0	# of Records: 22,408,258 %of Records: 100.0%

2018 Breaches Identified by the ITRC as of: 7/2/2018

Total Breaches: 668
Records Exposed: 22,408,258

The Identity Theft Resource Center breach database is updated daily and published to our website weekly. A US-based breach, as identified by our current process, is considered public when one of these occur:

1) Published by a credible source (sources include Offices of the Attorney General, and established media – TV news, radio, newspapers)

2) A letter notifying a potential victim has been received

ITRC will provide attribution of the source and include the relevant data to the extent that has been made public in our findings. If the number of records is not made publicly available, ITRC will note that in the report as "unknown" indicating we do not have the specifics of the actual number impacted. Identity Theft Resource Center reserves the right to make an educated estimate to the potential of impact based on our knowledge and understanding of the specifics of the policies of the reporting entity.



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

Report Date: 7/2/2018

Page 1 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-14	Palo Alto Unified School District	CA	2/14/2018	Electronic	Educational	Yes - Published #	353

Regrettably, we are writing to inform you that during an audit of our information storage practices on January 18, 2018, the District learned that an employee was storing confidential parent information on his laptop. (Type of information exposed per NY AG's office)

Attribution 1 Publication: NY AG's office Author:

Article Title: Palo Alto Unified School District

Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-13	Jay Zabel & Associates, LTD	IL	2/5/2018	Electronic	Business	Yes - Published #	191

Attribution 1 Publication: NY AG's office Author:

Article Title: Jay Zabel & Associates, LTD

Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-12	Metropolitan Life Insurance Company	NY	2/1/2018	Electronic	Business	Yes - Published #	335

After investigation, including communications with the policyholder and the policyholder's agent, we concluded that an unauthorized individual possessing the agent's account credentials (obtained from a source other than MetLife) had contacted MetLife in November 2017, posing as the agent and using the agent's credentials, to obtain a copy of the policyholder's MetLife policy application. This document included the policyholder's name, address, date of birth and Social Security number.

Attribution 1 Publication: NY AG's office Author:

Article Title: Metropolitan Life Insurance Company

Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-11	Trout, Ebersole & Groff LLP	PA	2/9/2018	Electronic	Business	Yes - Published #	620

On or about January 28, 2018, we discovered that we were the target of an e-mail phishing attack that resulted in the disclosure of your 2017 IRS Form W-2, Wage and Tax Statement. This information contained your first and last name, address, Social Security number and compensation information.

Attribution 1 Publication: NY AG's office Author:

Article Title: Trout, Ebersole & Groff LLP

Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-10	Investment Professionals, Inc.	TX	2/7/2018	Electronic	Banking/Credit/Financial	Yes - Published #	113

In November of 2016, two members of our company received a fraudulent email. Unfortunately, the user credentials for each person's company email account was compromised, and the mailboxes were accessible to a third party.

Attribution 1 Publication: NY AG's office Author:

Article Title: Investment Professionals, Inc.

Article URL: [Per FOIL NY AG's office](#)



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-09	Marshall & Sterling Insurance	NY	1/9/2018	Electronic	Business	Yes - Published #	101

On November 17, 2017, we learned that a Marshall & Sterling employee had inadvertently sent a tax form pertaining to your employer to a different Marshall & Sterling client. Upon learning of the issue, we commenced a prompt and thorough investigation. The information that was available on the tax form included your name, Social Security number and salary information.

Attribution 1 Publication: NY AG's office Author:
 Article Title: Marshall & Sterling Insurance
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-08	Remote DBA Experts, LLC	PA	2/1/2018	Electronic	Business	Yes - Published #	281

On January 17, 2018, an unauthorized individual impersonating an RDX executive emailed an RDX employee to request 2017 W-2 information for our employees. The data included your first name, last name, mailing address, Social Security number, and 2017 compensation and deduction information.

Attribution 1 Publication: NY AG's office Author:
 Article Title: Remote DBA Experts, LLC
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-07	DecisionHR	FL	1/12/2018	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that an employee clicked on a phishing email that appeared to be a legitimate business email. As a result, an unauthorized user accessed the employee's email account. Specifically, the email box included your first name, last name, social security number, and may have included your drivers' license number.

Attribution 1 Publication: NY AG's office Author:
 Article Title: DecisionHR
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-06	Capital One, NA	VA	1/10/2018	Electronic	Banking/Credit/Financial	Yes - Published #	1,991

On September 24, 2017, a call center agent employed at a vendor used by Capital One, N.A. ("Capital One") accessed your Credit Card account to make unauthorized changes against your account. 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, address, telephone number, date of birth, social security number, account number and account history. We are taking other steps to prevent this kind of event in the future.

Attribution 1 Publication: NY AG's office Author:
 Article Title: Capital One, NA
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-05	Seterus, Inc.	OR	1/18/2018	Electronic	Banking/Credit/Financial	Yes - Published #	101

On January 12, 2018, it was discovered Seterus had mailed borrower correspondence to the previous servicer, in error. This incident may have resulted in a disclosure of borrower name, loan number, property address, and loan details.

Attribution 1 Publication: NY AG's office Author:
 Article Title: Seterus, Inc.
 Article URL: [Per FOIL NY AG's office](#)



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-04	CyrusOne, Inc.	TX	1/8/2018	Electronic	Banking/Credit/Financial	Yes - Published #	402

On October 30, 2017, we learned that the permission setting to an HR-Payroll folder on a CyrusOne shared drive was inadvertently changed on October 18, 2017 to allow access to the folder to all CyrusOne employees and certain of our vendors.

Attribution 1 Publication: NY AG's office Author:
 Article Title: CyrusOne, Inc.
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-03	Broadview Mortgage Corporation	CA	1/30/2018	Electronic	Business	Yes - Published #	498

Per Notification NY AG's office
Description of Breach: Hacking
Information Acquired: Social Security number

Attribution 1 Publication: NY AG's office Author:
 Article Title: Broadview Mortgage Corporation
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-02	Beazer Homes	GA	1/12/2018	Electronic	Business	Yes - Published #	118

Beazer has learned that from approximately September 2017 through November 2017, an unknown person or persons remotely accessed and acquired without authorization emails belonging to certain Beazer employees. Type of exposed information not identified.

Attribution 1 Publication: NY AG's office Author:
 Article Title: Beazer Homes
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-01	Arthur Ventures Management, LLC	ND	1/12/2018	Electronic	Banking/Credit/Financial	Yes - Published #	210

On December 15, 2017, we learned that certain of your personal information could have been viewed as part of an email account compromise. You are receiving this notice because we recently learned that certain of your personal information could have been accessed, including your name, Social Security number and, for some individuals, driver's license number.

Attribution 1 Publication: NY AG's office Author:
 Article Title: Arthur Ventures Management, LLC
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180702-00	LJZ Enterprises, Inc. dba Sinatra's Restaurant	NY	2/13/2018	Electronic	Banking/Credit/Financial	Yes - Published #	5,369

A third party may have gained unauthorized access to data contained on the point of sale system of LJZ on November 27, 2016 (the "Breach"). The Breach, which was discovered on December 7, 2017, may have resulted in the hacker acquiring customer credit card and security code numbers.

Attribution 1 Publication: NH AG's office Author:
 Article Title: LJZ Enterprises, Inc. dba Sinatra's Restaurant
 Article URL: [Per FOIL NY AG's office](#)



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180701-09	Marion County Bank	IA	6/11/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Our investigation concluded that the unauthorized person did not have access to any bank or customer financial accounts and that no money was stolen. The email account that was compromised included a document with your name, address, bank account number, and social security number.

Attribution 1 Publication: IA AG's office Author:
 Article Title: Marion County Bank
 Article URL: https://www.iowaattorneygeneral.gov/media/cms/061118_Marion_County_Bank_51A8A08A7DFB6.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180701-08	Children's Mercy Hospital	MO	6/27/2018	Electronic	Medical/Healthcare	Yes - Published #	1,463

Children's Mercy Hospital MO Healthcare Provider 1463 06/27/2018 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
 Article Title: Children's Mercy 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
ITRC20180701-07	Tuskegee University	AL	6/22/2018	Electronic	Educational	Yes - Unknown #	Unknown

With the assistance of third-party forensic investigators, we learned Tuskegee was the victim of an email phishing attack which resulted in unauthorized access to certain faculty and staff email accounts between September 24, 2017 and March 22, 2018. It was recently determined that the information that could have been subject to unauthorized access includes name, address, Social Security number, financial account information, medical information, Driver's License number and credit or debit card number.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Tuskegee University
 Article URL: https://oag.ca.gov/system/files/CA-%20Notice%20of%20Data%20Event%20Packet_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180701-06	Regency Theaters	CA	6/19/2018	Electronic	Business	Yes - Unknown #	Unknown

At the beginning of June, we discovered that in January, 2018, information on the www.regencymovies.com website was accessed by an unauthorized third party. The information accessed was the information provided in utilizing the option of "Creating an Account" for ticket purchases on www.regencymovies.com. This includes; Name, Address, Email Address, Encrypted Passwords and Rewards Card Number.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Regency Theaters
 Article URL: https://oag.ca.gov/system/files/RegencyDataBreachAllClear_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180701-05	Hasbro, Inc.	RI	6/25/2018	Electronic	Business	Yes - Unknown #	Unknown

We became aware beginning on or around May 20, 2018 that an unauthorized party obtained access to certain of your personal data in shared network folders on Hasbro servers. Personal data that may have included your Social Security number, driver's license number, bank account number and/or routing number, credit card information, medical information, health insurance information, and/or passport number.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Hasbro, Inc.
 Article URL: https://oag.ca.gov/system/files/sample%20notices%20for%20ca-c%20%5B1930199_v1%5D_0.PDF

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180701-04	Amgen (Willis Towers Watson)	CA	6/26/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On April 23, 2018, we received a letter from WTW informing us that they had suffered a phishing incident that led to a breach of security and the potential unauthorized disclosure of personal information on February 21, 2018. The potential personal information involved included your: Name, Address, Phone Number, Date of the Incident you reported, Description of the Incident you reported, and, where a claim was paid, the amount that was paid. The Description of the Incident included a high-level description of the injury you may have suffered.

Attribution 1 Publication: CA AG's office Author:
Article Title: Amgen (Willis Towers Watson)
Article URL: https://oag.ca.gov/system/files/Amgen%20Data%20Subject%20Notice%20FINAL_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180701-03	East Bay Municipal Utility District (ersquared.org)	CA	6/27/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 25, 2018, staff learned that unauthorized individuals may have accessed ersquared.org, the third-party hosting environment for Marconi. The Marconi application database held some employee information, specifically: name, employee identification number, work email address, job title, and Marconi password hash (encrypted). As an emergency notification system, select employees had provided personal email address, home address, home phone number, and mobile phone number.

Attribution 1 Publication: CA AG's office Author:
Article Title: East Bay Municipal Utility District (ersquared.org)
Article URL: https://oag.ca.gov/system/files/062718%20Breach%20Notification_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180701-02	Alaska Department of Health and Social Services	AK	6/29/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

On April 26th, a DPA computer in the Northern region was infected with a Zeus/Zbot Trojan virus, resulting in breaches of the Health Insurance Portability and Accountability Act (HIPAA) and the Alaska Personal Information Protection Act (APIPA) involving more than 500 individuals. The computer had documents including information on pregnancy status, death status, incarceration status, Medicaid/Medicare billing codes, criminal justice, health billing, social security numbers, driver's license numbers, first and last names, birthdates, phone numbers, and other confidential data.

Attribution 1 Publication: sitnews.us Author:
Article Title: Northern Alaska Region HIPAA and APIPA Security Breach Notification
Article URL: http://www.sitnews.us/0618News/062918/062918_breach.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180701-01	Advanced Law Enforcement Rapid Response Training (AI FRRT)	TX	6/29/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

Personal data of thousands of law enforcement officials in the United States has been exposed in a security breach at a federally funded active shooter training center. Information included: •Over 85,000 emails sent by staff to prospective trainees and course takers dating back to at least 2011 were also stored; data on 65,000 officers who had taken an ALERRT course and provided feedback had their full name and zip code exposed; names of more than 17,000 instructors; and 51,345 sets of geolocation coordinates of schools, courts, police departments, and government buildings, like city halls and administrative offices.

Attribution 1 Publication: wccftech.com Author:
Article Title: Personal Data of Law Enforcement Officials Leaked by an Active Shooter Response Training Center
Article URL: <https://wccftech.com/active-shooter-response-exposes-data-police/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180628-03	L'Occitane, Inc. dba L'Occitane en Provence	NJ	6/21/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 25, 2018, L'Occitane discovered that unknown persons were attempting to gain unauthorized access to L'Occitane customer accounts on its U.S. website. L'Occitane immediately began an investigation and learned that these unknown persons appeared to be using account credentials, such as user logins and passwords, that were obtained from an unknown source in the hope that they might match the account credentials of L'Occitane's U.S. customers.

Attribution 1 Publication: NH AG's office Author:
Article Title: L'Occitane, Inc. dba L'Occitane en Provence
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/loccitane-20180621.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180628-02	New School Street Firehouse	NY	6/27/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

Records containing firefighters' personal information — including Social Security numbers, names, addresses and phone numbers — were found in the condemned firehouse in downtown Yonkers.

Attribution 1 Publication: lohud.com Author:
Article Title: Firefighter personnel records found tossed on floor of condemned Yonkers firehouse
Article URL: <https://www.lohud.com/story/news/local/westchester/yonkers/2018/06/27/yonkers-records-containing-personal-info-fo>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180628-01	David S. Ng, O.D.	CA	6/16/2018	Electronic	Medical/Healthcare	Yes - Published #	758

David S. Ng, O.D. CA Healthcare Provider 758 06/16/2018 Theft Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: David S. Ng, O.D.
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
ITRC20180627-06	Exactis	FL	6/27/2018	Electronic	Business	Yes - Unknown #	Unknown

Marketing and data aggregation firm Exactis may have exposed a database containing nearly 340 million individual records on a publicly accessible server, according to Wired. Highly personal information such as people's phone numbers, home and email addresses, interests and the number, age and gender of their children were reportedly exposed.

Attribution 1 Publication: cnet.com Author:
Article Title: Exactis: 340 million people may have been exposed in bigger breach than Equifax
Article URL: <https://www.cnet.com/news/exactis-340-million-people-may-have-been-exposed-in-bigger-breach-than-equifax/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180627-05	AH 2005 Management, LP	TX	6/7/2018	Electronic	Business	Yes - Unknown #	Unknown

As part of the investigation, it was determined that certain employee email accounts were subject to unauthorized access and certain emails were accessible to an unauthorized individual(s). On May 3, 2018, as part of the ongoing investigation, it was determined that certain personal information relating to certain individuals was in an accessible email. On May 25, 2018, it was determined that eight hundred twenty-seven (827) Iowa residents had the following information in an accessible email: Name and Social Security number.

Attribution 1 Publication: IA AG's office Author:
Article Title: AH 2005 Management, LP
Article URL: https://www.iowaattorneygeneral.gov/media/cms/060718_AH_2005_Management_LP_B75090AE65225.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180627-04	WellCare Health Plans, Inc.	FL	6/13/2018	Electronic	Medical/Healthcare	Yes - Published #	1,101

WellCare Health Plans, Inc. FL Health Plan 1101 06/13/2018 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: WellCare Health Plans, 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
ITRC20180627-03	New Jersey Department of Human Services	NJ	6/15/2018	Paper Data	Government/Military	Yes - Published #	1,263

New Jersey Department of Human Services NJ Health Plan 1263 06/15/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: New Jersey Department of Human 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
ITRC20180627-02	InfuSystem, Inc.	MI	6/22/2018	Electronic	Medical/Healthcare	Yes - Published #	3,882

InfuSystem, Inc. MI Healthcare Provider 3882 06/22/2018 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: InfuSystem, 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
ITRC20180627-01	Kelley Imaging Systems	WA	6/13/2018	Electronic	Medical/Healthcare	Yes - Published #	627

Kelley Imaging Systems WA Business Associate 627 06/13/2018 Hacking/IT Incident Desktop Computer, Electronic Medical Record, Network Server

Attribution 1 Publication: hhs.gov Author:
 Article Title: Kelley Imaging Systems
 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
ITRC20180626-07	Penn Mutual	PA	6/25/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On May 29, 2018, Penn Mutual discovered that certain client information may have been compromised when four of our insurance advisers account passwords were fraudulently reset by unauthorized third parties during the month of May 2018. The client information viewable from within the affected advisers' accounts included first and last name, date of birth, Penn Mutual account number, address, and the invoice amount paid for the Penn Mutual policy.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Penn Mutual
 Article URL: <http://ago.vermont.gov/blog/2018/06/25/penn-mutual-notice-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180626-06	The Hartford	CT	4/12/2018	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that personal information pertaining to your insurance claim was accessed by an unauthorized individual on or about [Date] in connection with our use of vendors to conduct medical review of claims. The documents accessed by the unauthorized individual contained your name together with medical information relating to your insurance claim and your Social Security number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180626-05	Advanced Technology Group, Inc.	OR	5/31/2018	Electronic	Business	Yes - Unknown #	Unknown

On April 30, 2018, evidence was discovered suggesting that certain .pdf attachments in a few user accounts may have been exposed during approximately a two week timeframe near the end of 2017 and may have contained personal information. On May 11, 2018, ATG determined that your personal information may have been exposed during this security incident. The affected information may have included your name, date of birth, phone number, home address, email address and social security number.

Attribution 1 Publication: MT AG's office Author:
Article Title: [Advanced Technology Group, Inc.](#)
Article URL: <https://dojmt.gov/wp-content/uploads/Advanced-Technology-Group.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180626-04	Humana.com and Go365.com	KY	6/21/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On June 3, 2018 Humana was the target of a sophisticated cyber spoofing attack that occurred on Humana.com and Go365.com. Your personal information on these websites may have been accessed by the attackers. Information potentially viewed/accessed could have included: medical, dental, and vision claims including services performed, provider name, dates of service, charge and paid amounts etc.; Spending account information such as health saving account spending and balance information, and Wellness information including biometric screening information

Attribution 1 Publication: MT AG's office Author:
Article Title: [Humana.com and Go365.com](#)
Article URL: https://dojmt.gov/wp-content/uploads/Humana-Go365.com_.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180626-03	Terteling Company, Inc.	ID	6/22/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 1, some employees received a phishing email that appeared to be a legitimate message from another employee and clicked on content in the email. The information that may have been accessible through this incident involves payroll and personal benefit data, including information pertaining to participation in our businesses' health plan. This data includes: first and last names, Social Security numbers, home addresses, birth dates, earnings amounts, and health plan ID numbers. Additionally, some email communications regarding health plan participation, coverage, or claims (including information concerning diagnoses, medications, procedures, treatment dates, and payments sought and paid) were potentially exposed in this incident.

Attribution 1 Publication: MT AG's office Author:
Article Title: [Terteling Company, Inc.](#)
Article URL: <https://dojmt.gov/wp-content/uploads/Terteling-Company-Inc..pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180626-02	Comcast - Xfinity	PA	5/22/2018	Electronic	Business	Yes - Unknown #	Unknown

It looks like a flaw in Comcast's website used for the activation of Xfinity routers can be exploited to harvest sensitive consumer information. "We were able to obtain their full address and ZIP code, which both customers confirmed," the publication reported. "The site returned the Wi-Fi name and password — in plain text — used to connect to the network for one of the customers."

Attribution 1 Publication: [PYMNTS.com](#) Author:
Article Title: [Comcast Faces Fallout From Website Bug That Leaked Consumer Data](#)
Article URL: <https://www.pymnts.com/news/security-and-risk/2018/comcast-xfinity-customer-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180626-01	Michigan Medicine	MI	6/25/2018	Electronic	Medical/Healthcare	Yes - Published #	871

On June 3, 2018, a Michigan Medicine employee's personal laptop computer was stolen. The theft occurred when the employee's car was broken into and his bag, which contained the laptop, was stolen. The data stored on the laptop varied based on the research studies, but could have included patient names, birthdates, medical record number, gender, race, diagnosis and other treatment-related information.

Attribution 1 Publication: University of Michigan website / hipaajou Author:
Article Title: Michigan Medicine notifies patients of health information data breach
Article URL: <https://www.uofmhealth.org/news/archive/201806/michigan-medicine-notifies-patients-health-information-data>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180625-06	K. Hovnanian American Mortgage, LLC	FL	4/2/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

A former employee may have accessed consumer data during her employment other than for the purposes of carrying out her assigned duties, during the time period between September, 2017 and February 2018. The information involved was loan application data, including names, social security numbers, dates of birth, addresses, credit and income information, as well as loan information.

Attribution 1 Publication: MD AG's office Author:
Article Title: K. Hovnanian American Mortgage, LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295017.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180625-05	US GreenFiber LLC	NC	4/3/2018	Electronic	Business	Yes - Published #	861

GreenFiber's computer system was compromised by a ransomware attack on February 12, 2018. The only personally identifiable information on the system was employee social security numbers and for a limited number of employees, driver's license number and/or biometric data. (Exposure number per IN AG's office)

Attribution 1 Publication: MD AG's office Author:
Article Title: US GreenFiber LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295127.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180625-04	HSBC Global Asset Management (USA) Inc.	NY	4/12/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 1, 2018 we became aware of an incident where an employee of HSBC sent an email on February 16, 2018 that inadvertently contained personally identifiable information for one customer to another HSBC client's email address. The information accessible included customer first and last name, account number(s) and share balance.

Attribution 1 Publication: MD AG's office Author:
Article Title: HSBC Global Asset Management (USA) Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295807.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180625-03	YMCA of the East Bay (The Redwoods Group, Inc.)	CA	4/27/2018	Electronic	Business	Yes - Unknown #	Unknown

On September 21, 2016, a thief stole the laptop computer of a Redwoods employee. While YMCA was a customer of Redwoods, YMCA provided information to Redwoods in relation to workers' compensation and legal claims asserted against YMCA

Attribution 1 Publication: CA AG's office Author:
Article Title: YMCA of the East Bay (The Redwoods Group, Inc.)
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297403.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180625-02	Brown, Lisle/Cummings, Inc.	RI	6/15/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 14, 2018, we completed our ongoing forensic investigation into a phishing incident and determined an unauthorized party may have accessed your personal information contained in the email account of one BLC employee. The information that could have been accessed in the affected accounts includes your name and Social Security number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Brown, Lisle/Cummings, Inc.
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/brown-lisle-20180615.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180625-01	PDQ	FL	6/22/2018	Electronic	Business	Yes - Unknown #	Unknown

We learned on June 8, 2018 that credit card information and or some names may have been hacked. Based on an investigation, the unauthorized access and or acquisition occurred from May 19, 2017 – April 20, 2018 (breach time period). We believe the attacker gained entry through an outside technology vendor's remote connection tool. The information accessed and or acquired included some or all of the following: names, credit card numbers, expiration dates, and cardholder verification value.

Attribution 1 Publication: PDQ website notice Author:
 Article Title: Important Information for our Guests On Data Breach
 Article URL: <https://www.eatpdq.com/promos/news/2018/06/22/questinfo>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-17	Taco John's of Iowa	IA	5/10/2018	Electronic	Business	Yes - Published #	6,012

As a result of the investigation, TJIA has determined that the server in question was compromised as the result of a phishing attack on or about July 14, 2017. The compromised server contained personal information about current and former employees, including name, address, telephone number, date of birth, compensation information, social security number and, if direct deposit was used by the employee, bank account number and bank routing number. (Exposure number per IN AG's office)

Attribution 1 Publication: IA AG's office Author:
 Article Title: Taco John's of Iowa
 Article URL: https://www.iowaattorneygeneral.gov/media/cms/051018_Taco_Johns_of_Iowa_4430BCF902146.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-16	Chalavoutis & Associates, LLC	NY	3/5/2018	Electronic	Business	Yes - Published #	497

Per Notification NY AG's office
 Description of Breach: Unauthorized access
 Information Acquired: Social Security number

Attribution 1 Publication: NY AG's office Author:
 Article Title: Chalavoutis & Associates, LLC
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-15	Iovance Biotherapeutics, Inc.	CA	3/1/2018	Electronic	Medical/Healthcare	Yes - Published #	116

As background, in July 2017, Iovance discovered that it was the victim of the unauthorized acquisition and theft of its confidential and proprietary data by its former Chief Medical Officer, Dr. Steven Fischkoff who had been terminated in March 2017.

Attribution 1 Publication: NY AG's office Author:
 Article Title: Iovance Biotherapeutics, Inc.
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-14	Novozymes US, Inc.	NC	2/15/2018	Electronic	Business	Yes - Published #	158

Per Notification NY AG's office
 Description of Breach: hacking
 Information Acquired: Social Security number

Attribution 1 Publication: NY AG's office Author:
 Article Title: Novozymes US, Inc.
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-13	SDI, Inc.	PA	3/2/2018	Electronic	Business	Yes - Published #	409

On February 12, 2018, SDI was the target of an email phishing scam that resulted in all 2016 and 2017 W-2 information being released outside the company. Based upon a review of the W-2s sent, the following information was involved: first and last name, address, Social Security number, and wage information. (Exposure number per IN AG's office)

Attribution 1 Publication: NY AG's office Author:
Article Title: SDI, Inc.
Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-12	Notre Dame de Namur University	CA	6/20/2018	Electronic	Educational	Yes - Unknown #	Unknown

On May 18, 2018, we learned that an unauthorized individual may have gained access to an employee's email account containing some of your personal information. Our investigation has determined that the affected email account contained a message with some of your personal information, which may include your name, Social Security number, and other information provided with your financial aid application.

Attribution 1 Publication: NH AG's office Author:
Article Title: Notre Dame de Namur University
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/notre-dame-20180620.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-11	Manchester Capital Management, LLC	VT	6/18/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

In May 2017, MCM's Montecito, California office was burglarized. The intruders vandalized the facilities and stole a piece of computer hardware along with some bicycles and other personal items belonging to MCM employees. The affected information may include names, account numbers, and social security numbers.

Attribution 1 Publication: NH AG's office Author:
Article Title: Manchester Capital Management, LLC
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/manchester-capital-20180618.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-10	Michael J. Duranceau, CPA, LLC	FL	6/1/2018	Electronic	Business	Yes - Unknown #	Unknown

We have recently learned that our firm's computer system was compromised by an outside attacker between the dates of April 2, 2018 to April 19, 2018. We did not know about this unauthorized access until it was reported to us on May 11, 2018 by a computer forensics company that was reviewing our system in response to some incidents in which tax returns were filed on behalf of some clients without authorization. In that regard, we believe it is possible that there was unauthorized access to your current and/or prior year tax returns and supporting documents, which included your name, address, date of birth, Social Security number, and/or financial account number(s).

Attribution 1 Publication: NH AG's office Author:
Article Title: Michael J. Duranceau, CPA, LLC
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/michael-duranceau-20180601.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-09	Health Management Concepts, Inc.	LA	6/11/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 25, 2018, we learned that a computer belonging to one of our employees was infected with ransomware. We conducted a thorough investigation of the ransomware incident and determined on April 30, 2018 that some of the files that may have been accessible to the attackers included files that contained your name and Social Security number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Health Management Concepts, Inc.
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/health-management-20180611.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-08	Humana	KY	6/4/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On January 17, 2018 a Humana contracted employee used an unapproved web application to transmit unsecured data as part of the Workday integration project. The personal information that was exposed included your name, social security number and home address.

Attribution 1 Publication: NH AG's office Author:
Article Title: Humana
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/humana-20180604.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-07	Educational Employees' Supplementary Retirement System of Fairfax County	VA	6/12/2018	Electronic	Business	Yes - Published #	3,332

ERFC forwarded to Master Print information containing the names, addresses, and Social Security numbers of those retirees to produce the mailing labels. Unfortunately, the Social Security numbers were included on the actual mailing labels above the names and addresses of the retirees. (Exposure number per WI AG's office)

Attribution 1 Publication: NH AG's office / WI AG's office Author:
Article Title: Educational Employees' Supplementary Retirement System of Fairfax County (Master Print)
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/educational-employees-20180612.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-06	Central Christian College of Kansas	KS	6/15/2018	Electronic	Educational	Yes - Unknown #	Unknown

Between July 11, 2017 and April 23, 2018, a student who sent an email to the group email received an email from the group participant. The email from the group participant contained a link to view the group. If a prospective or current student selected the option to view the group, the student could also view information that was submitted by other students. The affected information may have included the student's name, date of birth, phone number, home address, email address, social security number, and other information that the student submitted to the group mailbox.

Attribution 1 Publication: NH AG's office Author:
Article Title: Central Christian College of Kansas
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/central-christian-20180615.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-05	Citizens Financial Group	RI	6/14/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Citizens recently discovered that a person employed by one of our vendors engaged in unauthorized activity involving customer deposit accounts that resulted in fraudulent electronic transfers. Your name, social security number, account number and other information associated with your account may have been compromised.

Attribution 1 Publication: NH AG's office Author:
Article Title: Citizens Financial Group
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-20180614.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-04	Boston Biomedical, Inc.	MA	6/11/2018	Electronic	Medical/Healthcare	Yes - Published #	252

Upon discovery of a suspected Business Email Compromise attack, Boston Biomedical promptly activated its incident response plan, including engagement of a cybersecurity firm and cooperation with federal law enforcement. The information found in emails in the account included W-9, 1-9, and other employment forms, containing names, addresses, dates of birth, Social Security numbers, and in some cases passport numbers, along with other types of personal information of approximately 252 current and former employees and contractors.

Attribution 1 Publication: NH AG's office Author:
Article Title: Boston Biomedical, Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/boston-biomedical-20180611.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-03	Starr Insurance Holdings, Inc.	NY	5/24/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 18, 2018, Starr Insurance Holdings, Inc. ("Starr" or the company") determined certain information indicating that criminals may have gained access to an email account through a phishing attack and we promptly began an investigation. Personal information potentially involved in this incident may include: name, address, date of birth, Social Security number, driver's license, bank account number, passport number, insurance policy number or other insurance claim information.

Attribution 1 Publication: DE AG's office Author:
 Article Title: Starr Insurance Holdings, Inc.
 Article URL: <https://attorneygeneral.delaware.gov/wp-content/uploads/sites/50/2018/06/Starr-Insurance-Holdings-Sample-Notice.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180622-01	Firebase (Google)	CA	6/20/2018	Electronic	Business	Yes - Published #	4,050,000

The security issue, which the security firm refers to as the Firebase vulnerability, has a huge impact, leaking 100 million records (113 gigabytes) of data from unsecured Firebase databases. Analysis of the exposed data revealed 2.6 million plain text passwords and user IDs; more than 4 million Protected Health Information records (including chat messages and prescription details); 25 million GPS location records; 50 thousand financial records including banking, payment and Bitcoin transactions; and over 4.5 million Facebook, LinkedIn, Firebase and corporate data store user tokens.

Attribution 1 Publication: securityweek.com Author:
 Article Title: Thousands of Mobile Apps Leak Data from Firebase Databases
 Article URL: <https://www.securityweek.com/thousands-mobile-apps-leak-data-firebase-databases>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180621-07	Association for Supervision and Curriculum Development (ASCD)	VA	2/27/2018	Electronic	Business	Yes - Published #	192

Please be advised that on February 21, 2018, ASCD discovered it experienced an electronic/email communications scam intended to steal data, otherwise known as a "spearphishing attack". The personal information on a W-2 includes your name, address and social security number.

Attribution 1 Publication: NY AG's office Author:
 Article Title: Association for Supervision and Curriculum Development (ASCD)
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180621-06	Gwenn S Robinson MD	NM	6/14/2018	Electronic	Medical/Healthcare	Yes - Published #	2,500

Gwenn S Robinson MD NM Healthcare Provider 2500 06/14/2018 Hacking/IT Incident Desktop Computer

Attribution 1 Publication: hhs.gov Author:
 Article Title: Gwenn S Robinson 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
ITRC20180621-05	Black River Medical Center	MO	6/13/2018	Electronic	Medical/Healthcare	Yes - Published #	13,443

On April 23, 2018, we discovered that an employee's email account was compromised as the result of a phishing attack. The investigation determined that an unknown, unauthorized third party gained access to the employee's email account and could have viewed or accessed the information contained therein, which included patients' names, addresses and phone numbers, and in certain instances, limited treatment information.

Attribution 1 Publication: BRMC website / hipaajournal.com / hhs. Author:
 Article Title: BRMC NOTIFIES PATIENTS OF DATA SECURITY INCIDENT
 Article URL: <http://blackrivermedical.com/legal/brmc-notifies-patients-of-data-security-incident/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180621-04	Florida Agency for Persons with Disabilities	FL	6/1/2018	Electronic	Medical/Healthcare	Yes - Published #	1,951

The Florida Agency for Persons with Disabilities (FAPD), which provides support services for people with disabilities such as autism, cerebral palsy, spina bifida, and Downs syndrome, has experienced another phishing attack. The compromised email account contained information such as names, birth dates, addresses, telephone numbers, health information, and Social Security numbers.

Attribution 1 Publication: [hipaajournal.com / hhs.gov](#) Author:
Article Title: Further Phishing Attack Reported by Florida Agency for Persons with Disabilities
Article URL: <https://www.hipaajournal.com/florida-agency-for-persons-with-disabilities-and-black-river-medical-center-report-phish>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180621-03	Healthland Inc.	MN	6/10/2018	Electronic	Medical/Healthcare	Yes - Published #	614

Healthland Inc. MN Business Associate 614 06/10/2018 Unauthorized Access/Disclosure Other

Attribution 1 Publication: [hhs.gov](#) Author:
Article Title: Healthland 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
ITRC20180621-02	Dean Health Plan	WI	6/15/2018	Paper Data	Medical/Healthcare	Yes - Published #	1,311

Dean Health Plan WI Health Plan 1311 06/15/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: [hhs.gov](#) Author:
Article Title: Dean 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
ITRC20180621-01	RevUp Group, LLC	TN	6/20/2018	Electronic	Business	Yes - Unknown #	Unknown

An unauthorized user or users gained access to RevUp's system and installed one (or) more files that intercepted and stored our customer's data. The data at issue may have included certain RevUp customers' names, postal mailing addresses, email addresses, credit card numbers, credit card CVV numbers, and credit card expiration dates that were used during checkout for goods purchased through RevUp's Web site.

Attribution 1 Publication: [VT AG's office](#) Author:
Article Title: RevUp Group, LLC
Article URL: <http://ago.vermont.gov/blog/2018/06/20/revup-notice-of-security-incident-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180620-07	Hobe & Lucas CPA, Inc.	OH	2/15/2018	Electronic	Business	Yes - Unknown #	Unknown

On November 17, 2017, we discovered that an unknown individual gained access to an employee's email account. Although we do not believe it to be the case, it is possible that email correspondence between you and Hobe & Lucas CPA, Inc. may have contained your personal information, including your name, address, SSN, driver's license number and financial account information.

Attribution 1 Publication: [NY AG's office](#) Author:
Article Title: Hobe & Lucas CPA, Inc.
Article URL: [Per FOIL NY AG's office](#)



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180620-06	DiLeo & Charles Tax and Consulting Services, Inc.	NH	2/9/2018	Electronic	Business	Yes - Published #	118

Per Notification NY AG's office
 Description of Breach: hacking
 Information Acquired: Financial account information

Attribution 1 Publication: NY AG's office Author:
 Article Title: Dileo & Charles Tax and Consulting Services, Inc.
 Article URL:

Attribution 2 Publication: NY AG's office Author:
 Article Title: DiLeo & Charles Tax and Consulting Services, Inc.
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180620-05	Capital Integration Systems LLC (CAIS)	NY	3/31/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

The phishing attack was initiated through an email sent from a hacked email account at a trusted vendor and appeared legitimate, thereby deceiving the CAIS employee. It has been determined that the compromised account contained CAIS Shareholder names (or the name of the entity through which the shareholder invested in CAIS), tax identification numbers, postal addresses and email addresses.

Attribution 1 Publication: NY AG's office Author:
 Article Title: CAIS
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180620-04	Apple Bank for Savings (multiple locations)	NY	2/23/2018	Electronic	Banking/Credit/Financial	Yes - Published #	127

Per Notification NY AG's office
 Description of Breach: skimming
 Information Acquired: Financial account number

Attribution 1 Publication: NY AG's office Author:
 Article Title: Apple Bank for Savings
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180620-03	Amerifirst Home Mortgage	MI	3/28/2018	Electronic	Banking/Credit/Financial	Yes - Published #	887

Per Notification NY AG's office
 Description of Breach: Phishing email
 Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
 Article Title: Amerifirst Home Mortgage
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180620-02	American General Life Insurance Co. and US Life Insurance Co.	TX	2/27/2018	Electronic	Business	Yes - Published #	1,761

Per Notification NY AG's office
 Description of Breach: Inadvertent disclosure
 Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
 Article Title: American General Life Insurance Co. and US Life Insurance Co.
 Article URL: [Per FOIL NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180619-05	H-2 Enterprises, LLC	CO	4/2/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 5, 2018, it came to H-2 Enterprises' attention that the bank account number and bank routing number pertaining to one (1) business located in Maryland was accessed by an unauthorized intruder who had gained access to one employee email account through an email phishing attack.

Attribution 1 Publication: MD AG's office Author:
Article Title: H-2 Enterprises, LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295070.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180619-04	Gibbs & Cox	VA	4/9/2018	Electronic	Business	Yes - Unknown #	Unknown

Based on this investigation, we determined that in late November of 2017, the intruder(s) had gained access to a small number of employee email accounts. The intruder(s) accessed the employees' accounts via the public facing Outlook Web Access system. The personal information that was stored within an affected mailbox included your name, Social Security number, date of birth, and telephone number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Gibbs & Cox
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295843.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180619-03	Howard Bank	MD	4/9/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

In March of 2018, Howard Bank became aware of suspicious phishing email messages received by two of its employees and launched an investigation. The types of PII relating to Maryland residents determined to be stored within the impacted email accounts were not identical for every potentially affected individual, and they included the following: name, account number, and account balance information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Howard Bank
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295514%20\(1\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295514%20(1).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180619-02	Athena Consulting	MD	4/10/2018	Electronic	Business	Yes - Unknown #	Unknown

Athena Consulting was the victim of an email spoofing attack on February 20, 2018, by an individual pretending to be Athena Consulting's Chief Executive Officer. Unfortunately, copies of the 2017 employee W-2 forms were provided before the company discovered that the request was made from a fraudulent account by someone using the name and email address that appeared to be from Athena Consulting's CEO.

Attribution 1 Publication: MD AG's office Author:
Article Title: Athena Consulting
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295696.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180619-01	Betterton, Tyler & Summonte, P.L.	FL	4/10/2018	Electronic	Business	Yes - Unknown #	Unknown

Our investigation, that concluded on or about March 16, 2018, indicates that for a short window of time, beginning on or about February 12, 2018 and ending on or about February 14, 2018, hackers may have had the ability to access, copy, send and receive emails and contact information from this account. In any event, it is prudent to recognize that information, including names, social security numbers, driver's license numbers, and other personal identifiers, may have been compromised.

Attribution 1 Publication: MD AG's office Author:
Article Title: Betterton, Tyler & Summonte, P.L.
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295519%20\(1\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295519%20(1).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-11	Fox News LLC	NY	4/12/2018	Electronic	Business	Yes - Unknown #	Unknown

Specifically, we recently discovered that a corporate server that supports a Fox News expense reimbursement system was accessed by an unauthorized third party on or about March 13, 2018. Nonetheless, through our investigation we have determined that the third party may have gained access to user names and passwords that certain employees used to log in to the expense reimbursement system.

Attribution 1 Publication: MD AG's office Author:
Article Title: Fox News LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295678.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-10	ABC Phones of North Carolina, Inc. dba Victra	NC	4/13/2018	Electronic	Business	Yes - Unknown #	Unknown

After a detailed investigation, it was determined on March 13, 2018, that Victra had been the victim of a phishing scam and that two HR related employees' sharepoint environments may have been compromised.

Because of the nature of the breach, Victra believes that your personal information including the following may have been compromised: name, address, phone number, social security number, birth certificate, driver's license and other forms of government identifications, as well as earnings and financial information.

Attribution 1 Publication: MD AG's office Author:
Article Title: ABC Phones of North Carolina, Inc. dba Victra
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295811%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295811%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-09	Telestream, LLC	CA	4/25/2018	Electronic	Business	Yes - Published #	262

We are writing to inform you that Telestream, LLC learned on April 4, 2018 that it was the victim of an email phishing security incident which resulted in a breach of your personal information. Personal information that may be affected includes your name and social security number. (Exposure number per IN AG's office)

Attribution 1 Publication: MD AG's office Author:
Article Title: Telestream, LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297401.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-08	Missouri Athletic Club	MO	4/30/2018	Electronic	Business	Yes - Unknown #	Unknown

Through the investigation, which included working with third party forensic investigators, MAC learned it was the victim of an email phishing attack which affected certain employee email accounts. The investigation determined that the following information for certain Maryland residents was present in the impacted email accounts: name and payment card number, security code, and expiration date.

Attribution 1 Publication: MD AG's office Author:
Article Title: Missouri Athletic Club
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297384.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-07	City of Enumclaw	WA	2/16/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

We recently discovered that our City was the victim of an email spoofing attack by an individual pretending to be a member of City administration. The city of Enumclaw accidentally sent an email to an "individual pretending to be a member of City administration" and compromised the W-2s of hundreds of employees, records say. Unfortunately, copies of 2017 employee W-2 forms were provided before we discovered that the request was made from a fraudulent account.

Attribution 1 Publication: kiro7.com Author:
Article Title: Tax documents sent to scammer
Article URL: <https://www.kiro7.com/news/local/tax-documents-sent-to-scammer/701641370>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-06	Chicago Public Schools	IL	6/16/2018	Electronic	Educational	Yes - Unknown #	Unknown

Families were sent an email Friday evening from CPS's Office of Access and Enrollment inviting them to submit supplemental applications to selective enrollment schools. Attached at the bottom of the email was a link to a spreadsheet with the private data of over 3,700 students and families. The data includes children's names, home and cellphone numbers, emails and ID numbers.

Attribution 1 Publication: chicago.suntimes.com Author:
Article Title: CPS breach exposes private student data
Article URL: <https://chicago.suntimes.com/news/cps-data-breach-exposes-private-student-data/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-05	Veteran Affairs Medical Center	CA	6/18/2018	Electronic	Government/Military	Yes - Published #	1,030

A former employee of the Veteran Affairs Medical Center in Long Beach, CA who stole the protected health information (PHI) of more than 1,000 patients has been sentenced to three years in jail. A subsequent search of Torres' apartment revealed he had hard drives and zip drives containing the PHI of 1,030 patients and more than \$1,000 in cleaning supplies that had been stolen from the hospital.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Veteran Affairs Medical 3-Year Jail Term for VA Employee Who Stole Patient Data
Article URL: <https://www.hipaajournal.com/3-year-jail-term-for-va-employee-who-stole-patient-data/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-04	New England Baptist Health	MA	6/8/2018	Electronic	Medical/Healthcare	Yes - Published #	7,582

New England Baptist Health MA Healthcare Provider 7582 06/08/2018 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: New England Baptist 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
ITRC20180618-03	MyHeritage	US	6/15/2018	Electronic	Business	Yes - Unknown #	Unknown

On June 4, 2018, at 1 pm EST, we became aware of a data breach involving the email addresses and hashed passwords (these are not actual passwords) of 92.3 million MyHeritage users. We learned about the breach when MyHeritage's Chief Information Security Officer received a message from a security researcher, which stated that the researcher had found a file named myheritage containing email addresses and hashed passwords located on a private server outside of MyHeritage.

Attribution 1 Publication: CA AG's office / DE AG's office Author:
Article Title: MyHeritage
Article URL: https://oag.ca.gov/system/files/Consumer%20Notification_2.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-02	GreatBanc Trust Company	IL	6/15/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

For the first time in our history, during the week of October 23, 2017, we received indication that one of our computers was improperly accessed as the result of an email phishing scam. Based on that review we have determined that your personal information, such as name, address, date of birth and/or social security number, was contained in the email account.

Attribution 1 Publication: CA AG's office / NH AG's office / VT AG' Author:
Article Title: GreatBanc Trust Company
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_CA_0.PDF

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180618-01	POPSUGAR Inc.	CA	6/14/2018	Electronic	Business	Yes - Unknown #	Unknown

On April 30, 2018, we discovered that, in February 2018, an unauthorized third party gained access to account credentials and accessed certain user information. We have determined that the incident involved the following personal information regarding 123,857 website users: your name, email address, and hashed password.

Attribution 1 Publication: CA AG's office Author:
Article Title: POPSUGAR Inc.
Article URL: https://oag.ca.gov/system/files/POPSUGAR%20Notice%20of%20Data%20Breach_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180615-06	shopPOPdisplays (Miva Inc.)	NJ	6/11/2018	Electronic	Business	Yes - Unknown #	Unknown

We have been alerted by Miva Inc., which hosts our online order processing platform, that between April 8, 2018 and May 14, 2018 a malicious intruder inserted malware on Miva's servers supporting our online order processing platform. This could have included: address, email address, phone number, name, credit card number, credit card expiration date, and credit card CVV number.

Attribution 1 Publication: NH AG's office Author:
Article Title: shopPOPdisplays (Miva Inc.)
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/shopPOPdisplays-20180611.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180615-05	Qualified Plans, LLC	GA	6/6/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 11, 2018, we discovered that a small number of our employees' email accounts were the targets of a phishing attack that resulted in a compromise of their email credentials. However, our investigation revealed that the email contents within the two employee email accounts involved in this incident may have contained some of your personal information associated with the administration of your employee benefits, which may include your name, date of birth, and SSN.

Attribution 1 Publication: NH AG's office Author:
Article Title: Qualified Plans, LLC
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/qualified-plans-20180606.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180615-04	Med Associates, Inc.	NY	6/14/2018	Electronic	Medical/Healthcare	Yes - Published #	270,000

It was determined that the unauthorized party accessed the workstation and through that, may have had access to certain personal and protected information. While our investigation is ongoing, we have determined that the information that may have been accessible from the workstation included patient name, date of birth, address, dates of service, diagnosis codes, procedure codes and insurance information, including insurance ID Number.

Attribution 1 Publication: Med Associates, Inc. press release / NH Author:
Article Title: Med Associates Provides Notice of Data Security Incident
Article URL: <https://www.prnewswire.com/news-releases/med-associates-provides-notice-of-data-security-incident-300666812.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180615-03	Mountain House	NY	6/13/2018	Electronic	Business	Yes - Unknown #	Unknown

On April 12, someone hacked into the customer checkout page on the Mountain House website and installed computer code capable of capturing individual customer information as it was entered to complete online orders. This incident potentially involved the names, addresses, telephone numbers, email addresses, and credit card numbers and security codes of online customers who purchased Mountain House freezedried meals during this time period

Attribution 1 Publication: VT AG's office Author:
Article Title: Mountain House
Article URL: <http://ago.vermont.gov/blog/2018/06/13/ofd-foods-llc-notice-of-data-breach-to-consumers/>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180615-02	Ithaca College (3/8/18)	NY	6/13/2018	Electronic	Educational	Yes - Unknown #	Unknown

On March 8, 2018 Ithaca became aware of malware encryption of files on its London Center's server. Our investigation determined the following types of your personal information were stored within the impacted server and may have been viewed or downloaded by an unauthorized actor: driver's license number and name.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
 Article Title: Ithaca College (3/8/18)
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/ithaca-20180613.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180615-01	CHRISTUS Spohn Health System hospitals - Memorial and Shoreline	TX	6/15/2018	Electronic	Medical/Healthcare	Yes - Published #	1,800

A Christus Spohn employee was burgled on April 16, 2018 and PHI was taken including information such as names, birth dates, dates of service, medical record numbers, account numbers, ages, and other medical data.

Attribution 1 Publication: hipaajournal.com / kristv.com Author:
 Article Title: PHI Taken from Employee of Christus Spohn Hospitals
 Article URL: <https://www.hipaajournal.com/phi-stolen-in-san-francisco-and-corpus-christi-burglaries/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-14	HealthEquity Inc.	UT	6/13/2018	Electronic	Medical/Healthcare	Yes - Published #	23,000

On April 11, 2018, an unauthorized individual gained access to one email account for a HealthEquity employee. The spreadsheet contained your name, HealthEquity member ID, account type (e.g., HRA or FSA), deduction amount, and social security number. Your employer's name was contained in the email to which the spreadsheet was attached.

Attribution 1 Publication: VT AG's office / hipaajournal.com / Scm Author:
 Article Title: HealthEquity Inc.
 Article URL: <http://ago.vermont.gov/blog/2018/06/13/healthequity-inc-notice-of-data-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-13	University of Texas MD Anderson Cancer Center	TX	5/31/2018	Electronic	Medical/Healthcare	Yes - Published #	1,266

The University of Texas MD Anderson Cancer Center TX Healthcare Provider 1266 05/31/2018 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: University of Texas MD Anderson Cancer 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
ITRC20180614-12	Simply Well	TX	6/1/2018	Electronic	Medical/Healthcare	Yes - Published #	597

SimplyWell TX Business Associate 597 06/01/2018 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
 Article Title: Simply Well
 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
ITRC20180614-11	Massac County Surgery Center dba Orthopaedic Institute Surgery Center	IL	6/8/2018	Electronic	Medical/Healthcare	Yes - Published #	2,000

Massac County Surgery Center dba Orthopaedic Institute Surgery Center IL Healthcare Provider 2000 06/08/2018 Hacking/IT Incident Email



Attribution 1 Publication: hhs.gov Author:
 Article Title: Massac County Surgery Center dba Orthopaedic Institute 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
ITRC20180614-10	Medical Clinic of Houston, LLP	TX	5/22/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On March 23, 2018, we learned that a MCH staff member previously submitted your information to a pharmaceutical company for assistance with verifying your insurance benefits and eligibility for the drug Testopel. It appears that the information submitted to the pharmaceutical company may have included your name, address, date of birth, [Social Security number], health insurance policy and identification number, physician name, and clinical information related to your prescription for Testopel.

Attribution 1 Publication: MT AG's office Author:
 Article Title: Medical Clinic of Houston, LLP
 Article URL: <https://dojmt.gov/wp-content/uploads/Medical-Center-of-Houston.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-09	AAA Business Supplies	CA	6/13/2018	Electronic	Business	Yes - Unknown #	Unknown

Our accounting email addresses were compromised, which we discovered on Thursday, June 7, 2018. The parties involved appear to be pursuing fraudulent attempts to get AAA, our customers and our vendors to misdirect payments. The only information that was potentially exposed was information shared via email.

Attribution 1 Publication: CA AG's office Author:
 Article Title: AAA Business Supplies
 Article URL: https://oag.ca.gov/system/files/Confidential%20Security%20Alert_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-08	Weil, Akman, Baylin, & Coleman PA	MD	6/7/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 1, 2018, we learned that an unauthorized individual may have gained access to a small number of employee email accounts containing some of your personal information. Our investigation has determined that an affected email account contained a message with some of your personal information, including possibly your name, address, date of birth, Social Security number, driver's license number, financial account information, payment card information, or limited medical information.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Weil, Akman, Baylin, & Coleman PA
 Article URL: <http://ago.vermont.gov/blog/2018/06/07/weil-akman-baylin-coleman-pa-data-incident-notice-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-07	Evolution Hospitality (multiple properties)	CA	6/7/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 21, 2018, we identified unusual activity in an employee email account. We immediately changed the employee's credentials and launched an investigation, with the assistance of third-party forensic investigation firm, to determine what happened. As part of the investigation, we determined that certain employee email accounts were subject to unauthorized access and certain email were accessible to an unauthorized individual(s). Type of information exposed was not disclosed.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Evolution Hospitality (multiple properties)
 Article URL: <http://ago.vermont.gov/blog/2018/06/07/evolution-hospitality-llc-notice-of-data-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-06	Lutz & Carr CPAs, LLP	NY	6/7/2018	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you that we have been in contact with the IRS because some of our clients received a letter from the Internal Revenue Service asking to verify their identity. We have confirmed with the IRS that returns being filed by our clients are not being monitored, and that clients who received this letter filed tax returns matching certain criteria used by the IRS in the identity verification process.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Lutz & Carr CPAs, LLP
Article URL: <http://ago.vermont.gov/blog/2018/06/07/lutz-carr-cpas-llp-informational-notice-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-05	Total Phase, Inc.	CA	6/8/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 29, 2018, Total Phase discovered that it had been the victim of a cyber attack. Cyber attackers installed unauthorized code on our website to harvest information from customers' web browsers during the checkout process on Total Phase's website. This information included your name, billing and shipping addresses, credit card number, expiration date and CVV, company name, and phone number. Your Total Phase username and password may also have been compromised if they were entered on the checkout page during the impacted time period.

Attribution 1 Publication: VT AG's office Author:
Article Title: Total Phase, Inc.
Article URL: <http://ago.vermont.gov/blog/2018/06/08/total-phase-inc-security-incident-notice-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-04	Wilkins, Reinicke and Company PC	CO	6/8/2018	Electronic	Business	Yes - Unknown #	Unknown

On April 24, 2018, we discovered that our computer systems had been impacted by a ransomware attack. Although the investigation determined that the ransomware simply encrypted files, it is possible that your name, address, Social Security number and other tax information may have been viewed or accessed by an unauthorized third party.

Attribution 1 Publication: VT AG's office Author:
Article Title: Wilkins, Reinicke and Company PC
Article URL: <http://ago.vermont.gov/blog/2018/06/08/wilkins-reinicke-co-pc-notice-of-data-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-03	Weichert Company	NJ	6/11/2018	Electronic	Business	Yes - Unknown #	Unknown

On December 20, 2017, during the conduct of a risk assessment review, we discovered that a data file server may have been accessible by unknown individuals. We immediately took action, removing the server, and conducted an investigation to determine what information was at risk of compromise. We determined that certain client real estate transactions containing your name, address, and Social Security number were contained on the server.

Attribution 1 Publication: VT AG's office Author:
Article Title: Weichert Company
Article URL: <http://ago.vermont.gov/blog/2018/06/11/weichert-co-data-security-incident-letter-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-02	Highgate Hotels, LP	TX	6/11/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 3, 2018, we learned that an unauthorized individual may have gained access to an employee's email account containing some of your personal information. Our investigation has determined that the affected email account contained a message with some of your personal information, including possibly your name, address, payment card number, and financial account number.

Attribution 1 Publication: VT AG's office Author:
Article Title: Highgate Hotels, LP
Article URL: <http://ago.vermont.gov/blog/2018/06/11/highgate-hotels-lp-information-incident-notice-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180614-01	Denise M. Bowden, Lac, MS	CA	6/11/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On April 30, 2018, Ms. Bowden discovered that her office had been burglarized and a computer was stolen. The password protected computer contained patients' names, addresses and contact information, and itemized receipts that included dates of service, diagnosis codes and procedure codes.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Denise M. Bowden, Lac, MS
 Article URL: https://oag.ca.gov/system/files/NYDOCS01-%239077761-v1-Denise-Bowden---AG-Notification-Letter---CA_0.PDF

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180613-10	Benefit Outsourcing Solutions	MI	6/7/2018	Electronic	Medical/Healthcare	Yes - Published #	1,144

Benefit Outsourcing Solutions MI Business Associate 1144 06/07/2018 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
 Article Title: Benefit Outsourcing 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
ITRC20180613-09	H&R Block	MO	5/9/2018	Electronic	Business	Yes - Unknown #	Unknown

Documents from the H&R Block tax office at 920 151h SW Suite102 Auburn, WA 98001 were recently being transferred to a secure storage facility, and during this process the transport vehicle along with all the documents inside the vehicle were stolen by one or more criminals. The stolen documents contained confidential information belonging to you and/or others included on your tax return. Information on the documents may have included name, address, phone number, Social Security Number and other tax-related information.

Attribution 1 Publication: WA AG's office Author:
 Article Title: H&R Block
 Article URL: https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Home/Supporting_Law_Enforcement/HRBlock.2018-05-09

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180613-08	Walgreens	IL	6/5/2018	Electronic	Business	Yes - Unknown #	Unknown

On April 17, 2018, Walgreens discovered unauthorized skimming devices attached to a point-of-sale pin pad in two Nashville Rite Aid locations owned and operated by Walgreens, specifically at 2416 West End Avenue and 700 Gallatin Road. The skimming devices may have captured the following information: your credit or debit card number; the PIN associated with the debit card, if one was used; and possibly your first and last name.

Attribution 1 Publication: VT AG's office / MT AG's office Author:
 Article Title: Walgreens
 Article URL: <http://ago.vermont.gov/blog/2018/06/05/walgreen-co-fraudulent-alert-notice-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180613-07	Stein Eriksen Lodge Hotel	UT	6/1/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 22, 2018, Stein Eriksen Lodge Hotel (the "Hotel") learned that your personal information may have been subject to unauthorized access or acquisition as the result of a cyber-attack. The data element involved may have included name, address, birthdate, and Social Security number.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Stein Eriksen Lodge Hotel
 Article URL: <http://ago.vermont.gov/blog/2018/06/01/stein-eriksen-lodge-hotel-data-incident-notice-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180613-06	Temecula Motorsports, Inc.	CA	5/31/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 30, 2018, Temecula learned of a potential data security incident involving the unauthorized installation of malware on our e-commerce web platform. The affected payment card information may have included names, card numbers, expiration dates, and security codes.

Attribution 1 Publication: VT AG's office Author:
Article Title: Temecula Motorsports, Inc.
Article URL: <http://ago.vermont.gov/blog/2018/05/31/temecula-motorsports-inc-notice-of-data-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180613-05	Cactus Wellhead, LLC	TX	5/17/2018	Electronic	Business	Yes - Published #	1,086

Cactus Wellhead, LLC greatly values you as an employee and respects the privacy of your information, which is why we are writing to inform you that we recently learned that certain of your personal information was released as part of an associate's response to a phishing email directed to the company by someone impersonating a senior member of management. This incident took place on May 9, 2018 and resulted in the unauthorized release of your Form W2 for 2017, which contained your name, address, and social security number. (Exposure number per IN AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180613-04	Crius Energy, LLC	CT	5/18/2018	Electronic	Business	Yes - Unknown #	Unknown

Regrettably, we are writing to inform you that after a forensic investigation, which included manual review of thousands of documents, we confirmed on April 27, 2018 that some of your personal information may have been accessible to a hacker as a result of a sophisticated e-mail phishing attack that occurred on or around January 22, 2018. The personal information that may have been accessible through the phishing incident included names, dates of birth, and driver's license numbers. Additionally, some Social Security numbers may have been included in some documents that were accessible to the attacker.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180613-03	International Management Advisors, Ltd.	OH	5/18/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On Thursday, April 26, 2018, International Management Advisors, Ltd. ("IMA") received an e-mail purporting to be from a valid entity and claiming to require action in response to suspicious activity on the account. While the types of personal information contained in the compromised account and computer may vary from person to person, in general such information may include for any affected individual name, address, phone number, e-mail address, date of birth, social security number, driver's license or other government-issued identification number, financial account information, health insurance information and other data that may constitute personal information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180613-02	Service Employees International Union (SEIU) Local 32BJ	NY	5/25/2018	Electronic	Business	Yes - Unknown #	Unknown

A 32BJ employee was the victim of an email phishing attack via an externally-hosted email management system, resulting in unauthorized access to emails during a 24-hour period from November 13-14, 2017. The impacted email account contained your full name and Social Security number.

Attribution 1 Publication: MT AG's office / DE AG's office Author:
Article Title: Service Employees International Union (SEIU) Local 32BJ
Article URL: <https://dojmt.gov/wp-content/uploads/32BJ.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180613-01	Quad-C Management, Inc.	VA	6/7/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Quad-C Management, Inc. recently learned that an unauthorized individual may have illegally accessed a Quad-C employee's email account. The information the unauthorized individual may have accessed is used to facilitate your investment activity and includes your social security number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180612-09	Juilliard School	NY	4/18/2018	Electronic	Educational	Yes - Unknown #	Unknown

We recently learned that your IRS Form 1042-S was mailed to an incorrect address. We corrected the process issue that caused this and recently re-sent the form to your correct address. The information contained on your 1042-S includes your name, address, and Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Juilliard School
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-296785.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180612-08	Hepburn and Sons LLC	VA	4/19/2018	Electronic	Business	Yes - Unknown #	Unknown

As most of you know, we recently had a company-wide breach regarding tax information that has caused delays in your returns. The source was a very sophisticated phishing technique from international criminals using Microsoft 365 look alike credentials. We believe that these criminals did gain access to all our 2016 and 2017 W2s.

Attribution 1 Publication: MD AG's office Author:
Article Title: Hepburn and Sons LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297396.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180612-06	Premier Fixtures, LLC	NY	4/19/2018	Electronic	Business	Yes - Published #	855

On March 9, 2018, Premier learned through an ongoing forensic investigation into a phishing incident that an unauthorized party obtained access to several email accounts belonging to Premier employees. Type of information exposed was not disclosed. (Exposure number per IN AG's office)

Attribution 1 Publication: MD AG's office Author:
Article Title: Premier Fixtures, LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-296814.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180612-05	American Society of Anesthesiologists	IL	4/20/2018	Electronic	Business	Yes - Published #	819

On March 8, 2018, our client discovered an external "phishing" attempt on its email system. The personal information subject to unauthorized access during the breach included the names, email addresses, and social security numbers of our client's employees and dependents of employees. (Exposure number per IN AG's office)

Attribution 1 Publication: MD AG's office Author:
Article Title: American Society of Anesthesiologists
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297322%20\(1\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297322%20(1).pdf)



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180612-04	Friends of Falls Church	VA	4/20/2018	Electronic	Business	Yes - Unknown #	Unknown

We have just learned that several donors to the Friends of Falls Church (Virginia) Homeless Shelter ("FFCHS") were recent victims of banking fraud which involved electronic copies of paper checks written to FFCHS in December 2017. In an abundance of caution, we have notified all donors who made paper check donations in December 2017 that were included in the January 2, 2018 deposit, that this incident may have exposed some of their personal information that was included on their paper checks, including name, address, bank account number, and signature.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Friends of Falls Church
 Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-296819%20\(1\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-296819%20(1).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180612-03	UniCarriers Americas Corporation	IL	4/23/2018	Electronic	Business	Yes - Unknown #	Unknown

On or about April 2, 2018 we discovered that ransomware had infected several employee files on or about March 31, 2018. Affected employees' personal information including names, addresses, and Social Security numbers may have been accessed.

Attribution 1 Publication: MD AG's office Author:
 Article Title: UniCarriers Americas Corporation
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297398.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180612-02	Signature Systems Group, LLC	TX	4/24/2018	Electronic	Business	Yes - Published #	228

During the investigation, we determined a limited number of company email accounts were logged into by an unauthorized actor between February 2 and February 10, 2018, likely as the result of email phishing attacks that stole employee email account credentials. The types of PII relating to the impacted individuals determined to be stored in the impacted email accounts included two or more of the following data elements: name, Social Security number, bank account number, credit card number, or health insurance information. (Exposure number per IN AG's Office)

Attribution 1 Publication: MD AG's office Author:
 Article Title: Signature Systems Group, LLC
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297331.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180612-01	Ramy Brook LLC	NY	4/24/2018	Electronic	Business	Yes - Published #	328

As background, this incident involved malware that was placed onto our site, allowing an unauthorized third party to access transaction-related information during the period of March 8, 2018 and April 17, 2018 consisting of purchasers' names, e-mails, mailing/billing addresses, and credit card numbers, expiration dates and CVV numbers. (Exposure number per IN AG's Office)

Attribution 1 Publication: MD AG's office Author:
 Article Title: Ramy Brook LL
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297328.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-24	PrintingCenterUSA.com	MT	5/29/2018	Electronic	Business	Yes - Unknown #	Unknown

During recent review of our website and systems we discovered some suspicious code that may have been present on our website at times from January 2018 through May 9, 2018. We believe that this code was a result of activity relating to one of our vendors. This code may have had the ability to capture some customer account logon and payment card information as it was entered by customers into our website forms and shopping pages, but before PrintingCenterUSA.com received it on our systems.

Attribution 1 Publication: NH AG's office / VT AG's office Author:
 Article Title: PrintingCenterUSA.com
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/printingcenterusa-20180529.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-23	St. Mary's Health, Inc. dba St. Vincent Evansville	IN	6/5/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On February 15, 2018, during preliminary investigation under the incident response protocol (IRP), we identified a configuration error on the server that exposed the data within the credentialing software application to the internet. Information on the impacted server that may have been downloaded could include your: Name, Address, Date of birth, Phone number, Driver's license, Social Security Number, National Provider Data Bank report.

Attribution 1 Publication: VT AG's office Author:
 Article Title: St. Mary's Health, Inc. dba St. Vincent Evansville
 Article URL: <http://ago.vermont.gov/blog/2018/06/05/st-marys-health-inc-security-notification-letter-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-21	Blue Cross Blue Shield of Illinois (Dane Street)	IL	6/6/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On 04/09/2018, Dane Street, a vendor of Blue Cross Blue Shield of Illinois, learned from law enforcement that a doctor providing peer reviews for Dane Street was accused of fraudulently impersonating another doctor in order to perform medical peer reviews. The data that may have been seen by this individual during the peer review process includes your name, address, phone number, date of birth, social security number and medical service information.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Blue Cross Blue Shield of Illinois
 Article URL: <http://ago.vermont.gov/blog/2018/06/06/blue-cross-and-blue-shield-of-illinois-notice-of-data-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-20	BioIQ Inc.	CA	5/25/2018	Electronic	Medical/Healthcare	Yes - Published #	4,059

BioIQ Inc. CA Business Associate 4059 05/25/2018 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: BioIQ 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
ITRC20180611-19	Dino-Peds	CO	5/30/2018	Electronic	Medical/Healthcare	Yes - Published #	1,357

Dino-Peds CO Healthcare Provider 1357 05/30/2018 Unauthorized Access/Disclosure Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
 Article Title: Dino-Peds
 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
ITRC20180611-18	University of Utah Health	UT	6/2/2018	Electronic	Medical/Healthcare	Yes - Published #	607

University of Utah Health UT Healthcare Provider 607 06/02/2018 Theft Laptop, Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
 Article Title: University of Utah 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
ITRC20180611-17	Capitol Anesthesiology	TX	6/1/2018	Electronic	Medical/Healthcare	Yes - Published #	2,231

Capitol Anesthesiology Association TX Healthcare Provider 2231 06/01/2018 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Capitol Anesthesiology
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
ITRC20180611-16	RISE Wisconsin, Inc.	WI	6/7/2018	Electronic	Medical/Healthcare	Yes - Published #	3,731

Rise Wisconsin is alerting more than 3,700 plan members that some of their protected health information was potentially accessed by unauthorized individuals during a recent ransomware attack. Potentially, the types of data that could have been accessed by the attackers includes names, addresses, dates of birth, Social Security numbers and, for certain patients, a limited amount of health information.

Attribution 1 Publication: hipaajournal.com / hhs.gov / WI AG's off Author:
Article Title: 3,700 Rise Wisconsin Plan Participants Potentially Impacted by Ransomware Attack
Article URL: <https://www.hipaajournal.com/3700-rise-wisconsin-plan-participants-potentially-impacted-by-ransomware-attack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-15	Terros Health	AZ	6/8/2018	Electronic	Medical/Healthcare	Yes - Published #	1,600

Officials with Terros Health say a data breach has possibly compromised personal information of more than one thousand of its patients. The news release said a phishing attack allowed a person or group to access a company email account. Patients' name, date of birth, physical and email address, diagnosis, medical records number and "other protected health information" may have been exposed.

Attribution 1 Publication: www.abc15.com / kjzz.org / hipaajournal Author:
Article Title: Terros Health data breach: 1,600 patients potentially impacted
Article URL: <https://www.abc15.com/news/region-phoenix-metro/central-phoenix/terros-health-data-breach-1600-patients-potential>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-14	Manduka (3/27/2018)	CA	3/27/2018	Electronic	Business	Yes - Published #	64,270

On February 25, 2018, Manduka learned of a potential data security incident involving the unauthorized installation of malware on our e-commerce web platform. web platform to purchase products from February 22, 2017 to March 5, 2018. The affected payment card information may have included names, card numbers, expiration dates, and security codes. (Exposure number per IN AG's Office)

Attribution 1 Publication: NH AG's office Author:
Article Title: Manduka (3/27/2018)
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/manduka-20180327.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-13	Forever 21 (Willis Towers Watson)	CA	6/1/2018	Electronic	Business	Yes - Unknown #	Unknown

Forever 21 was recently notified by our insurance broker, Willis Towers Watson ("WTW"), that an unauthorized third-party obtained access to two of WTW's employees' email accounts between February 15, 2018 and March 23, 2018. The summary documents in WTW's employees' email accounts contained information related to your claim(s), including your name, date(s) of injury, information about your injury(es), and claim(s) amount(s).

Attribution 1 Publication: CA AG's office Author:
Article Title: Forever 21 (Willis Towers Watson)
Article URL: https://oag.ca.gov/system/files/F21%20Sample%20CA%20Claimant%20Notice%20Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-12	Hair Free Forever	CA	6/3/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Unfortunately, one of our former employees; Nathalie Collins, stole personal and confidential information from our patient's files and data base, which is a violation of HIPAA and other privacy laws. This includes names, addresses, phone numbers, email, birth dates and Medical Information regarding individual's medical history, mental or physical condition, medical treatment or diagnosis by a health care professional, names of doctors, medications, illness and intimate personal photographs.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Hair Free Forever
Article URL: https://oag.ca.gov/system/files/Notice%20of%20Data%20Breach_1.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-11	Edward D. Jones & Co, L.P. (PricewaterhouseCoopers LLP)	MO	6/4/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On April 26, 2018, we were informed that PricewaterhouseCoopers LLP ("PwC"), which maintains some of our clients' information to provide tax services to Edward Jones, mistakenly provided a file containing some of our clients' information to another financial services company via a secure, encrypted online portal. The information disclosed included full names and tax identification numbers, including Social Security numbers.

Attribution 1 Publication: CA AG's office Author:
Article Title: Edward D. Jones & Co, L.P. (PricewaterhouseCoopers LLP)
Article URL: https://oag.ca.gov/system/files/LGL-11189-A_FINAL_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-10	PLAE, Inc.	CA	6/4/2018	Electronic	Business	Yes - Unknown #	Unknown

As a security best practice, we do not store customer financial data in our systems but this particular attack involved scraping information entered in real-time from website visitors during the above time period. Based on what we know now, personal information that may have been compromised as a result included names, addresses, telephone numbers, emails, credit card numbers and related security codes.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: PLAE, Inc.
Article URL: https://oag.ca.gov/system/files/PLAE%20Notification%20Letter%20-%2020052918%20FINAL_for%20state%20regulators_

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-09	9W Halo OpCo L.P. dba Angelica	GA	6/7/2018	Electronic	Business	Yes - Unknown #	Unknown

On April 10, 2018, Angelica sent an email to a former employee in response to his request for a copy of his 2017 W-2. Instead of sending only the former employee's 2017 W-2, the response inadvertently included an attachment with 2017 W-2 forms for multiple current and former employees of Angelica, including you. The W-2 information included your name, address, Social Security Number, and earnings information from 2017.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: 9W Halo OpCo L.P. dba Angelica
Article URL: https://oag.ca.gov/system/files/Angelica%20-%20Sample%20Notification%20Letter%20for%20California%201_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-08	Aimbridge Hospitality Holdings, LLC	TX	6/7/2018	Electronic	Business	Yes - Unknown #	Unknown

As part of the investigation, it was determined that certain employee email accounts were subject to unauthorized access and certain emails were accessible to an unauthorized individual(s). On May 25, 2018, it was determined that thirteen thousand four hundred and seventy-eight (13,478) California residents had one or more of the following in an accessible email: Name, Social Security number, financial account information, or username and password.

Attribution 1 Publication: CA AG's office Author:
Article Title: Aimbridge Hospitality Holdings, LLC
Article URL: <https://oag.ca.gov/system/files/Aimbridge%20Hospitality%20Holdings%2C%20LLC%20-%20Notice%20of%20Data%20E>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-07	Systeme Software, Inc.	PA	6/7/2018	Electronic	Business	Yes - Unknown #	Unknown

Although Systeme has no information to suggest that any unauthorized individual acquired access to that server, Systeme later determined that Google's search engine "crawled" the server, making the documents searchable for a brief period of time. After reviewing the files that were on the server at issue, we have determined that the information contained on the "results files" may have consisted of individual names, and in some cases individuals' addresses, telephone numbers and/or Social Security numbers.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Systeme Software, Inc.
 Article URL: <https://oag.ca.gov/system/files/LEGAL%2036547669v1%20Systeme%20-%20State%20AG%20Notice%20-%20California>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-06	Manduka (6/8/18)	CA	6/8/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 20, 2018, Manduka learned of a potential data security incident involving the unauthorized installation of malware on our e-commerce web platform. The affected payment card information may have included names, card numbers, expiration dates, and security codes.

Attribution 1 Publication: CA AG;s office Author:
 Article Title: Manduka (6/8/18)
 Article URL: https://oag.ca.gov/system/files/Manduka%20Round%202%20Ad%20r1prf_1.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-05	Melissa James, EA, LLC	LA	5/9/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 26, 2018, we discovered that certain customer information was acquired without authorization. The incident may have involved names and Social Security numbers.

Attribution 1 Publication: MT AG's office Author:
 Article Title: Melissa James, EA, LLC
 Article URL: <https://dojmt.gov/wp-content/uploads/Melissa-James-Bookkeeping-Tax.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-04	Elmcroft Senior Living, Inc.	OR	6/1/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 10, 2018, an unauthorized third party accessed our servers which included files containing personal information about you or your family member. The third party may have accessed demographic data and personal health information about you or your family member, including your or your family member's name, date of birth, address, and in some instances, a social security number.

Attribution 1 Publication: CA AG's office / hipaajournal.com / DE Author:
 Article Title: Elmcroft Senior Living, Inc.
 Article URL: https://oag.ca.gov/system/files/Elmcroft%20-%20Ad%20-%20206.1.18%20final_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-03	Transamerica	NY	6/1/2018	Electronic	Business	Yes - Unknown #	Unknown

We recently discovered unauthorized access to your retirement plan online account information available through the Transamerica Retirement Solutions website that may have occurred between March, 2017 and January, 2018. The affected information may have included your name, address, Social Security number, date of birth, financial account information, and employment details.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Transamerica
 Article URL: https://oag.ca.gov/system/files/Individual%20Notice%20Letter_2.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-02	Bay Area Air Quality Management District	CA	5/25/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

On January 10, 2018, unknown individuals accessed an Air District email account and gained access to messages sent to and from that account over a period of approximately two weeks. The data accessed included the Social Security Numbers of current and former employees and several past and present members of the Board of Directors, Hearing Board and Advisory Council maintained by the Air District for record keeping purposes. Additionally, a significantly smaller number of Social Security Numbers, Driver's License Numbers, Credit Card Numbers, Medical Information, and Health Insurance Information from various individuals was included in individual messages, much of which was regarding the individuals whose email accounts were compromised.

Attribution 1 Publication: CA AG's office Author:
Article Title: Bay Area Air Quality Management District
Article URL: https://oag.ca.gov/system/files/20180525%20BAAQMD%20Sample%20Breach%20Notice_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180611-01	TVShowsonDVD	CA	5/24/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 21, 2018, we determined that between January and May 2018, an unauthorized party had gained access to information submitted by users to TVShowsonDVD. As a result, certain registration information that you submitted to the site, which may have included your name, username, password, or date of birth, may have been compromised.

Attribution 1 Publication: CA AG's office / DE AG's office Author:
Article Title: TVShowsonDVD
Article URL: https://oag.ca.gov/system/files/Sample%20Notice%20of%20Security%20Breach_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-13	Uno Alla Volta, LLC Inc.	CT	5/22/2018	Electronic	Business	Yes - Published #	1,121

An investigation confirmed that a network intruder had installed malicious code on our website that allowed the intruder to obtain access to certain personal information provided by customers on our website during the period the code was active, beginning on April 18th and ending on May 1, 2018 when the code was identified and immediately disabled. The incident involved customer names and addresses as well as credit card numbers, CCV#s, and expiration dates. (Exposure number per IN AG's Office)

Attribution 1 Publication: NH AG's office / VT AG's office Author:
Article Title: Uno Alla Volta, LLC Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/uno-alla-20180522.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-12	Luxury Retreats	US	5/24/2018	Electronic	Business	Yes - Published #	345

On May 10, 2018, Luxury Retreats concluded its investigation into the nature and extent of a security incident, including the identification of potentially affected individuals, after learning on March 22, 2018, that an unknown individual had gained access to an employee's corporate email account. The investigation identified certain customer personal information in the email account that was provided in connection with booking a villa - which varied by customer but may have included name, address, date of birth, payment card account number, external verification code (CVV), financial account number, driver's license number, and passport number. (Exposure number per IN AG's Office)

Attribution 1 Publication: NH AG's office / VT AG's office Author:
Article Title: Luxury Retreats
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/luxury-retreats-20180524.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-11	Jarrett & Luitjens, PLC	VT	5/24/2018	Electronic	Business	Yes - Unknown #	Unknown

On April 19, 2018, a duplicate backup drive that contained firm files was dropped in our office parking lot during our routine drive exchange and is presumed stolen by a passerby who was seen retrieving the drive. Out of an abundance of caution, we are sending this notice to all past and current clients, regardless of whether the drive contains their sensitive information, as well as to any other individuals who may have provided us with personally identifiable information, such as a name, address, date of birth and Social Security number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Jarrett & Luitjens, PLC
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/jarrett-20180524.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-10	Fidelity Investments	MA	5/22/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Due to an administrative error, Fidelity inadvertently granted another investment advisory firm access to your account from March 17, 2018 to May 7, 2018. Information about the account, including your name, Social Security number, date of birth, account number, positions, balances and transaction history, was available to the other advisory firm and included in secure daily transmissions to the firm's third-party portfolio management system.

Attribution 1 Publication: NH AG's office Author:
Article Title: Fidelity Investments
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/faithfulness-20180522.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-09	Employee Benefits Corporation	WI	5/22/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 7, 2018, Employee Benefits Corporation became aware of unusual FedEx tracking emails, which took the form of a typical phishing email, received by certain participants of a small number of benefit plans administered by Employee Benefits Corporation. In addition to your name, the database may contain the following information about you: email address, Social Security number, phone number, mailing address, date of birth, and in limited circumstances, financial account information and healthcare related information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Employee Benefits Corporation
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/employee-benefits-20180522.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-08	Dignity Health (Healthgrades)	CA	5/31/2018	Electronic	Medical/Healthcare	Yes - Published #	55,947

In a Dignity Health statement emailed to HealthITSecurity.com, the healthcare provider explained that an email list formatted by its business associate Healthgrades contained a sorting error that resulted in misaddressed emails being sent to a group of patients about an online appointment scheduling tool. The misdirected email contained the wrong patient's name and his or her physician's name.

Attribution 1 Publication: hhs.gov / healthitsecurity.com Author:
Article Title: Dignity Health Data Breach Affects 55.9K Patients
Article URL: <https://healthitsecurity.com/news/dignity-health-data-breach-affects-55.9k-patients>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-07	John A. Moran Eye Center at the University of Utah	UT	6/2/2018	Electronic	Medical/Healthcare	Yes - Published #	607

The Moran Eye Center learned a laptop computer and an associated external storage device used to take and store retinal images were stolen April 3 from locked storage at 65 Mario Capecchi Drive in Salt Lake City. The stolen equipment stored retinal images, full or partial names, dates of birth and medical reference numbers used to identify records within the University of Utah Health medical records system.

Attribution 1 Publication: Heraldextra.com Author:
Article Title: Moran Eye Center reports theft, possible data breach
Article URL: https://www.heraldextra.com/news/local/moran-eye-center-reports-theft-possible-data-breach/article_c58e782f-6293-5c

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-06	Family Health Clinic of Carroll County	IN	5/25/2018	Electronic	Medical/Healthcare	Yes - Published #	112

As the investigation moved into May, the security team found malware also had been installed on a computer used to scan health insurance cards at the affiliated Family Health Clinic of Carroll County, a group practice, around mid-March. Analysis of the infected computer at Family Health Clinic of Carroll County found at-risk data could have included patient names, health insurance information, driver's license numbers and Medicare numbers.

Attribution 1 Publication: healthdatamanagement.com / hhs.gov Author:
Article Title: Family Health Clinic of Carroll County
Article URL: <https://www.healthdatamanagement.com/news/two-breaches-at-purdue-university-affect-more-than-1-700-patients>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-05	Purdue University Pharmacy	IN	5/25/2018	Electronic	Medical/Healthcare	Yes - Published #	1,599

Purdue University Pharmacy found an unauthorized remote access file had been installed on pharmacy systems, putting some patient data at risk. The Purdue breach potentially compromised protected health information that included patient names, patient identification numbers, diagnoses, treatments, and amounts billed and paid.

Attribution 1 Publication: [healthdatamanagement.com / hhs.gov](#) Author:
 Article Title: [Purdue University Pharmacy](#)
 Article URL: <https://www.healthdatamanagement.com/news/two-breaches-at-purdue-university-affect-more-than-1-700-patients>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-04	TicketFly, Inc.	CA	6/1/2018	Electronic	Business	Yes - Unknown #	Unknown

As many of you are aware, Ticketfly.com has been the target of a cyber incident. We have learned that some customer information has been compromised as part of the incident, including names, addresses, emails, and phone numbers of Ticketfly fans.

Attribution 1 Publication: [Ticketfly notice](#) Author:
 Article Title: [TicketFly, Inc.](#)
 Article URL: <https://support.ticketfly.com/customer/en/portal/articles/2941983-ticketfly-cyber-incident-update>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-02	Philips	MA	5/24/2018	Electronic	Business	Yes - Unknown #	Unknown

The incident which occurred in May 2018 was caused by an unknown actor sending an email to the employees' work email account which requested the employee to click on a link and reveal their personnel account log-in credentials ("phishing incident"). The personal information that was the subject of the phishing incident included name and financial account information in electronic format.

Attribution 1 Publication: [NH AG's office](#) Author:
 Article Title: [Philips](#)
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/philips-20180524.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180604-01	Pendleton Square Trust Company	TN	5/25/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 3, 2018, we learned that an unauthorized source gained access to an email account potentially containing sensitive information. This could have included names, addresses, dates of birth, social security numbers or driver's license numbers.

Attribution 1 Publication: [VT AG's office](#) Author:
 Article Title: [Pendleton Square Trust Company](#)
 Article URL: <http://ago.vermont.gov/blog/2018/05/25/pendleton-square-trust-company-notice-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180529-03	Aflac	GA	5/25/2018	Electronic	Business	Yes - Published #	10,396

Based on our review, Aflac email accounts of a small number of our independent contractor insurance agents appear to have been accessed by an unauthorized third party. Based on our review, the information in the accounts may have included the following: first and last name, home address, date of birth, policy/certificate number, group number, type of policy (such as life, hospital and dental), Social Security number (SSN) and bank account information.

Attribution 1 Publication: [Aflac website](#) Author:
 Article Title: [Aflac](#)
 Article URL: <https://www.aflac.com/docs/hipaa-notice-2018.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180529-02	Holland Eye Surgery and Laser Center	MI	5/18/2018	Electronic	Medical/Healthcare	Yes - Published #	42,200

According to a statement to this site: in June, 2016, he hacked Holland Eye Surgery & Laser Center in Holland, Michigan. He then reportedly contacted them and demanded a "security fee" of \$10,000.00 for helping them secure their patient data. That database has names, addresses, insurance information, and some other fields.

Attribution 1 Publication: [databreaches.net / hhs.gov](#) Author:
Article Title: [Holland Eye Surgery and Laser Center](#)
Article URL: <https://www.databreaches.net/mi-holland-eye-surgery-laser-center-notifies-42200-patients-about-2016-hack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180529-01	Care Partners Hospice and Palliative	OR	5/25/2018	Electronic	Medical/Healthcare	Yes - Published #	600

A Hillsboro hospice center is warning patients that a recent security breach may have allowed the personal health information of patients to fall into the wrong hands. That investigation, led by a third-party cybersecurity company, indicates that emails from the account may have been accessed without authorization. The company said the private health information of some patients may have been accessed.

Attribution 1 Publication: [hipaajournal.com / portlandtribune.com](#) Author:
Article Title: [Hillsboro hospice service warns of data breach](#)
Article URL: <http://portlandtribune.com/ht/117-hillsboro-tribune-news/396672-290691-hillsboro-hospice-service-warns-of-data-brea>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-11	University of Vermont (NetID)	VT	5/25/2018	Electronic	Educational	Yes - Unknown #	Unknown

On Wednesday, UVM notified users of NetID, a portal that grants access to campus email, services such as class registration and even final grades, that the "intrusion" could lead to malicious use of usernames and passwords. Corredera said UVM is working with police and information security experts to investigate the breach and has asked NetID users to be "extra vigilant" and report suspicious activity.

Attribution 1 Publication: [mychamplainvalley.com](#) Author:
Article Title: [UVM warns faculty, students of potential breach of personal data](#)
Article URL: <http://www.mychamplainvalley.com/news/local-news/uvm-warns-faculty-students-of-potential-breach-of-personal-data>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-10	Pinnacle Advisory Group, Inc.	MD	5/21/2018	Electronic	Banking/Credit/Financial	Yes - Published #	1,706

On March 27, 2018, Pinnacle learned that a Pinnacle employee email account was accessed without authorization. The following information may have been affected: your name, date of birth, Social Security number or Taxpayer Identification number, and financial account numbers. (Exposure number per IN AG's Office)

Attribution 1 Publication: [NH AG's office](#) Author:
Article Title: [Pinnacle Advisory Group, Inc.](#)
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/pinnacle-advisory-20180521.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-09	Integrated Practice Solutions, Inc.	CA	5/22/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On February 1, 2018, IPS learned that because of a configuration error, certain links used by patients and chiropractic practices to access IPS's SmartCloud platform were exposed and made searchable on the internet. Based on IPS's extensive forensic investigation to date, which included a leading outside forensics firm expert in these matters, the information contained in the compromised links may have included: full name; Social Security Number; address; date of birth; medications; care provider; medical history and other health information.

Attribution 1 Publication: [NH AG's office](#) Author:
Article Title: [Integrated Practice Solutions, Inc.](#)
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/integrated-practice-20180522.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-08	D.C. Department of Health	DC	5/24/2018	Electronic	Government/Military	Yes - Published #	600

The D.C. Department of Health has warned hundreds of nurses that their personal information was inadvertently exposed in the online licensing portal and is offering them one year of credit-monitoring services. A nurse navigating the nursing board's online portal somehow ended up on a nonpublic portion of a database that included the Social Security numbers, names and addresses of nurses, said Department of Health spokesman Tom Lalley.

Attribution 1 Publication: washingtonpost.com Author:
Article Title: D.C. government data breach exposed nurses' Social Security numbers
Article URL: <https://www.washingtonpost.com/local/dc-politics/dc-government-data-breach-exposed-nurses-social-security-numbe>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-07	AgentRun	IL	5/24/2018	Electronic	Business	Yes - Unknown #	Unknown

A software startup that provides independent insurance brokers with customer management software has exposed highly sensitive information on thousands of insurance policy holders. The data included detailed insurance policy documents containing names, postal addresses, dates of birth, and phone numbers. In some cases there were also documents revealing an income range, ethnicity, and marital status. Many of the documents were scans of people's identification documents, including Social Security cards and numbers, Medicare cards, and other documents, such as driver licenses, and armed forces and voter identification cards

Attribution 1 Publication: zdnet.com Author:
Article Title: Insurance startup leaks sensitive customer health data
Article URL: <https://www.zdnet.com/article/insurance-startup-leaks-sensitive-customer-health-data/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-06	Monroe County Clerk / Department of Motor Vehicles	NY	5/25/2018	Paper Data	Government/Military	Yes - Unknown #	Unknown

County Clerk's Office tossed personal, sensitive customer information in the trash. The papers included renewal applications with names, addresses and social security numbers which we blacked out, the Homeland Security and Visa information of an exchange student at UofR, boat registration stickers and stacks of 10 day car inspection tags.

Attribution 1 Publication: whec.com Author:
Article Title: County Clerk's Office tossing personal, sensitive customer information in the trash
Article URL: <http://www.whec.com/news/dmv-tossing-personal-sensitive-customer-information-in-the-trash/4921799/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-05	California Department of Public Health	CA	5/23/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

On March 12, 2018, a vehicle belonging to a CDPH contractor, who performs health facilities inspections, was broken into and some documents and a laptop were stolen. The information involved may have included your first and last name, date of birth, Social Security number, address, diagnoses and other health information, health insurance information, and demographic information.

Attribution 1 Publication: CA AG's office Author:
Article Title: California Department of Public Health
Article URL: https://oag.ca.gov/system/files/Sample%20CDPH%20Breach%20Notification%20Letter_5_23_18_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-04	Golden 1 Credit Union	CA	5/22/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On April 24, 2018, we discovered your payment card information and personal identification number (PIN) may have been compromised during its usage at an ATM machine at a Golden 1 branch in Roseville.

Attribution 1 Publication: CA AG's office Author:
Article Title: Golden 1 Credit Union
Article URL: https://oag.ca.gov/system/files/Sample%20Notice%20of%20Data%20Breach_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-03	T-Mobile	WA	5/24/2018	Electronic	Business	Yes - Unknown #	Unknown

The subdomain, which can be easily found on search engines, contained a hidden API that would return T-Mobile customer data simply by adding the customer's cell phone number to the end of the web address. Although the API is understood to be used by T-Mobile staff to look up account details, it wasn't protected with a password and could be easily used by anyone. The returned data included a customer's full name, postal address, billing account number, and in some cases information about tax identification numbers. The data also included customers' account information, such as if a bill is past-due or if the customer had their service suspended. The data also included references to account PINs used by customers as a security question when contacting phone support.

Attribution 1 Publication: zdnet.com Author:
Article Title: T-Mobile bug let anyone see any customer's account details
Article URL: <https://www.zdnet.com/article/tmobile-bug-let-anyone-see-any-customers-account-details/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-02	Aultman Health Foundation	OH	5/25/2018	Electronic	Medical/Healthcare	Yes - Published #	42,625

Aultman Health Foundation, which runs Aultman Hospital in Canton, OH, is notifying approximately 42,600 patients that some of their protected health information may have been compromised as a result of a phishing attack. Email accounts used by Aultman hospital and certain physician practices contained names, addresses, clinical information, medical record numbers, and physicians' names. Individuals tested by AultWorks Occupational Medicine had a greater range of information exposed including name, address, date of birth, medical history, reports on physical examinations, the results of drug, hearing, and breathing tests, and other lab test results.

Attribution 1 Publication: hipajournal.com / cantonrep.com / hhs. Author:
Article Title: UPDATE: 42,600 patients affected by data breach at Aultman
Article URL: <https://www.hipajournal.com/42600-patients-potentially-impacted-by-aultman-health-foundation-phishing-attack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180525-01	Echo Canyon Healthcare, Inc. dba Heritage Court Post Acute of Scottsdale	AZ	5/21/2018	Paper Data	Medical/Healthcare	Yes - Published #	1,765

Echo Canyon Healthcare, Incorporated dba Heritage Court Post Acute of Scottsdale AZ Healthcare Provider 1765 05/21/2018 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Echo Canyon Healthcare, Inc. dba Heritage Court Post Acute of Scottsdale
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
ITRC20180524-03	Dignity Health	NV	5/10/2018	Paper Data	Medical/Healthcare	Yes - Published #	6,036

Dignity Health Healthcare Provider 6036 05/10/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Dignity Health - St. Rose Dominican, Siena, and DeLima Hospitals
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
ITRC20180524-01	Coca-Cola Company	GA	5/23/2018	Electronic	Business	Yes - Published #	8,000

On September 1, 2017, we were informed by law enforcement officials that a former employee of a Coca-Cola subsidiary was found in possession of an external hard drive containing information that appeared to have been misappropriated from Coca-Cola. Type of information exposed was not disclosed. (Exposure number of records per <https://www.bleepingcomputer.com/news/security/coca-cola-suffers-breach-at-the-hands-of-former-employee/>)

Attribution 1 Publication: VT AG's office / bleepingcomputer.com / Author:
Article Title: Coca-Cola Company
Article URL: <http://ago.vermont.gov/blog/2018/05/23/coca-cola-company-notice-of-data-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180523-06	Equias Alliance, LLC	CA	5/8/2018	Electronic	Business	Yes - Published #	2,264

On February 27, 2018, Equias confirmed through its ongoing forensic investigation that a phishing incident occurred where emails and attachments from two employee e-mail accounts may have potentially been accessed by an unauthorized person. Type of information exposed was not disclosed. (Exposure number per IN AG's Office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180523-05	Muir Medical Group	CA	5/22/2018	Electronic	Medical/Healthcare	Yes - Published #	5,485

On March 7, 2018, we discovered that a former employee of Muir IPA took with her certain information in the possession of Muir IPA before her employment ended with Muir IPA in December 2017. The information taken by Muir IPA's former employee may have included your personal information, including demographic information (such as your name, address, email address, telephone number, date of birth, and Social Security number to the extent your Medicare number is derived from your Social Security number), insurance information (such as your health insurance plan name and health insurance identification number), and clinical information (such as your diagnoses, test results, medication information, and other treatment information in Muir IPA's possession).

Attribution 1 Publication: CA AG's office / hipaaajournal.com / hhs Author:
Article Title: Muir Medical Group
Article URL: https://oag.ca.gov/system/files/Patient%20Notice%20Template%20%28002%29_0.PDF

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180523-04	Hancock County Board of Developmental Disabilities	OH	5/17/2018	Paper Data	Business	Yes - Published #	607

Hancock County Board of Developmental Disabilities OH Healthcare Provider 607 05/17/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Hancock County Board of Developmental Disabilities
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
ITRC20180523-03	New York City Human Resources Administration/Department of Social Services	NY	5/11/2018	Paper Data	Government/Military	Yes - Published #	2,078

New York City Human Resources Administration/Department of Social Services NY Health Plan 2078 05/11/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: New York City Human Resources Administration/Department of Social 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
ITRC20180523-02	Humana	KY	5/21/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Recently we received a number of calls to several of our automated Humana 1-800 numbers (Interactive Voice Response (IVR) Telephone System) that our technology team determined were suspicious. The information that was used for identification in our IVR system was Humana member identification number or Social Security Number, date of birth and ZIP code.

Attribution 1 Publication: VT AG's office Author:
Article Title: Humana
Article URL: <http://ago.vermont.gov/blog/2018/05/21/humana-notice-of-data-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180523-01	Associates in Psychiatry and Psychology	MN	5/18/2018	Electronic	Medical/Healthcare	Yes - Published #	6,546

Rochester, MN-based Associates in Psychiatry and Psychology (APP) has experienced a ransomware attack that affected several computers containing patients' protected health information. The types of information potentially accessed includes names, birth dates, addresses, Social Security numbers, insurance information, and treatment records.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: More than 6,500 Patients Potentially Impacted by Minnesota Ransomware Attack
Article URL: <https://www.hipaajournal.com/more-than-6500-patients-potentially-impacted-by-minnesota-ransomware-attack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180521-10	Central Islip Union Free School District	NY	2/13/2018	Electronic	Educational	Yes - Published #	1,362

On February 1, 2018, Central Islip Union Free School District ("the District") learned of a potential data incident which may have resulted in unauthorized access to your personal information. It appears if the contents were placed in a certain way within the envelope and the envelope was tapped in various ways it may have permitted some information to be viewable through the envelope's window. The data elements involved may have included name, address, and Social Security number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Central Islip Union Free School District
Article URL: [Per FOIL Request NY AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180521-09	North America Administrators, L.P.	TN	5/11/2018	Electronic	Business	Yes - Unknown #	Unknown

Through its investigation, NAA determined that an unauthorized individual may have accessed certain emails and attachments in a small number of NAA employees' email accounts between the dates of January 7, 2018 and January 24, 2018 through a phishing email scheme. The investigation further determined that emails and attachments in the employees' email accounts may have contained information about group health plan members, including names, Social Security numbers, medical information, and/or health insurance information.

Attribution 1 Publication: NH AG's office Author:
Article Title: North America Administrators, L.P.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/north-america-20180511.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180521-08	University of Toledo	OH	5/16/2018	Electronic	Business	Yes - Published #	6,094

On January 16, 2018, we learned that a University of Toledo faculty member misplaced an unencrypted flash drive. The information that was available on the flash drive included your name, address, and Social Security number, and may have also included your date of birth.

Attribution 1 Publication: NH AG's office Author:
Article Title: University of Toledo
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/university-of-toledo-20180516.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180521-07	ViaTech Publishing Solutions	MN	4/10/2018	Paper Data	Medical/Healthcare	Yes - Published #	3,327

ViaTech Publishing Solutions, Inc. MN Health Plan 3,327 04/10/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: ViaTech Publishing 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
ITRC20180521-06	TeenSafe	CA	5/20/2018	Electronic	Business	Yes - Unknown #	Unknown

At least one server used by an app for parents to monitor their teenagers' phone activity has leaked tens of thousands of accounts of both parents and children. The database stores the parent's email address associated with TeenSafe, as well as their corresponding child's Apple ID email address. It also includes the child's device name -- which is often just their name -- and their device's unique identifier. The data contains the plaintext passwords for the child's Apple ID.

Attribution 1 Publication: zdnet.com Author:
Article Title: Teen phone monitoring app leaked thousands of user passwords
Article URL: <https://www.zdnet.com/article/teen-phone-monitoring-app-leaks-thousands-of-users-data/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180521-05	University at Buffalo	NY	5/19/2018	Electronic	Educational	Yes - Unknown #	Unknown

Thousands of UB community members' account information have been hacked. On Friday, UB confirmed that J. Brice Bible, vice president and chief information officer, is investigating and responding to a breach of external third-party accounts that comprised the login information for 2,690 UBITName accounts.

Attribution 1 Publication: UofB school publication Author:
Article Title: University at Buffalo
Article URL: <http://www.ubspectrum.com/article/2018/05/ub-logins-stolen-in-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180521-04	Los Angeles County 211	CA	5/18/2018	Electronic	Government/Military	Yes - Published #	33,000

The nonprofit organization that operates Los Angeles County's social services hotline inadvertently exposed personal information that was stored online, according to county officials and a private security firm that discovered the vulnerability. Chris Vickery, director of UpGuard's cyber risk research team, said the information he discovered included names, email addresses and weakly encrypted passwords of users operating the 211 system, potentially opening them to attack. The data also contained records for 3.5 million calls and a substantial amount of personally identifiable information, Vickery said. That included 33,000 Social Security numbers, and in many cases full names and addresses — as well as detailed notes for 200,000 calls logged between 2010 and 2016.

Attribution 1 Publication: www.techwire.net Author:
Article Title: LA County CIO Probing Data Breach; CISO Expands Inquiry
Article URL: <https://www.techwire.net/news/la-county-cio-probing-data-breach-ciso-calls-it-innocuous.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180521-03	Corporation Service Company	DE	5/17/2018	Electronic	Business	Yes - Published #	94,148

During routine security monitoring, we detected that an unauthorized third party accessed parts of our network and certain systems. While the investigation into this event is ongoing, the data stored with the exfiltrated database table included a combination of the individuals' names and Social Security numbers or credit card/debit card information. (Exposure number per IN AG's Office)

Attribution 1 Publication: CA AG's office / NH AG's office / VT AG' Author:
Article Title: Corporation Service Company
Article URL: https://oag.ca.gov/system/files/CSC-%20California%20Notice%20of%20Data%20Event_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180521-02	Black Phoenix, Inc.	CA	5/17/2018	Electronic	Business	Yes - Published #	150

I have lousy news to share: some time between May 1st and May 16th, the Black Phoenix Alchemy Lab site was hacked. Information that could have been accessed without authorization could have included your name, credit card billing address, telephone number, email address, and credit card number data, the name on card, expiration date, and security code.

Attribution 1 Publication: CA AG's office Author:
Article Title: Black Phoenix, Inc.
Article URL: https://oag.ca.gov/system/files/NOTICE%20OF%20DATA%20BREACH%20-%20BP_0.pdf



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180521-01	Bombas, LLC	NY	5/18/2018	Electronic	Business	Yes - Published #	41,000

Malware in the code of the e-commerce platform was identified and initially removed from our website on January 15, 2015, and then finally removed on February 9, 2015. The data accessed may have included personal information such as name, address, and credit card information.

Attribution 1 Publication: CA AG's office / VT AG's office Author:
 Article Title: Bombas, LLC
 Article URL: https://oag.ca.gov/system/files/Bombas%20Ad%20r4prf%20%28002%29_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-15	Pension Fund of the Christian Church	IN	1/16/2018	Electronic	Business	Yes - Published #	10,981

On December 18, 2017, Pension Fund learned that a password protected employee laptop had been stolen from a locked car and that the laptop contained certain personal information of members, including name, address, social security number, account number and member identification number.

Attribution 1 Publication: NC AG's office Author:
 Article Title: Pension Fund of the Christian Church
 Article URL: [Per FOIA Request NC AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-14	Marriott International	MD	2/22/2018	Electronic	Business	Yes - Unknown #	Unknown

Specifically, on February 5, 2018, we discovered that between January 23, 2018 and February 5, 2018, a third party obtained unauthorized access to employee information by false pretenses. Through our investigation, we have determined that the third party had access to the employees' direct deposit information, pay statement and W2 information.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Marriott International
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295059.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-13	Principal Financial Group	IA	2/28/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

The purpose for our letter is to notify you that your personal information was included in a contribution report, which was sent to an incorrect plan sponsor of ours on January 31, 2018. The contribution report contained your personal information, including your name, Social Security number, and the dollar amount of any contributions made to your account in the plan between October 1, 2017 and January 30, 2018.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
 Article Title: Principal Financial Group
 Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295079%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295079%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-12	State Employee Credit Union of Maryland	MD	3/2/2018	Electronic	Banking/Credit/Financial	Yes - Published #	554

We have discovered that a few of our ATMs were recently compromised using an unauthorized electronic device, commonly known as a skimmer. A third party or parties may have obtained unauthorized debit or ATM card information, including payment card information and the associated personal identification number (PIN), at a few of our ATMs.

Attribution 1 Publication: MD AG's office Author:
 Article Title: State Employee Credit Union of Maryland
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295145.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-11	Parkway Corporation	PA	3/2/2018	Electronic	Business	Yes - Published #	589

Beginning on February 14, 2018, requests were made from what appeared to be a legitimate Parkway email requesting Parkway employee W-2 information. A file sent in response to the fraudulent email included the following information related to certain Parkway employees: (1) name; (2) Social Security number; (3) wage information; and (4) amounts paid for state, federal, and local taxes. (Number of Records exposed per NC AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office / NC AG Author:
Article Title: Parkway Corporation
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295144.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-10	Remington Hotels, LLC	TX	3/2/2018	Electronic	Business	Yes - Published #	313

On February 1, 2018, we learned that a document with Remington employees' W-2 information mistakenly was provided to an unauthorized individual. We have verified that your W-2 information, including your first name, last name, income information and social security number mistakenly was provided to an unauthorized individual. (Exposure number per IN AG's Office)

Attribution 1 Publication: MD AG's office Author:
Article Title: Remington Hotels, LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295143.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-09	Fairchild Maddox & Leonidas, Ltd.	MN	3/2/2018	Electronic	Business	Yes - Published #	2,365

We are writing to inform you of a data security incident at Fairchild Maddox + Leonidas that may have resulted in the disclosure of your personal information, including your name and Social Security number. As a result of our investigation, we determined that your personal information, including your name, address, date of birth, Social Security number, and financial account information may have been accessed. (Number of Records exposed per NC AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office / NC AG Author:
Article Title: Fairchild Maddox & Leonidas, Ltd.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295142.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-08	Waccamaw Management, LLC	SC	3/5/2018	Electronic	Business	Yes - Unknown #	Unknown

On February 27, 2018, Waccamaw Management was the target of an email phishing scam when an employee received a request that appeared to be from a Waccamaw Management executive, requesting copies of employees' wage and tax statements. The documents sent included your name, address, Social Security Number and income information for 2017.

Attribution 1 Publication: MD AG's office Author:
Article Title: Waccamaw Management, LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295169.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-07	Personal Care Products Council	DC	3/7/2018	Electronic	Business	Yes - Published #	128

On February 24, 2016, a copy of a spreadsheet containing personal information pertaining to PCPC employees was erroneously misdirected internally to a PCPC employee not generally authorized to access this information. The spreadsheet contained information including the name, address, date of birth, social security number, dates of employment, compensation, and benefits information belonging to 33 current and former employees residing in Maryland. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Personal Care Products Council
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295201%20\(1\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295201%20(1).pdf)



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-06	M&E Tax and Financial Services	VA	3/6/2018	Electronic	Business	Yes - Published #	1,810

Please be advised, our client, M&E Tax and Financial Services ("M&E") suffered a potential data security incident as the result of a ransomware attack which occurred on December 12, 2017. M&E is providing this notification as its systems contain data elements of personal information for its clients including name, address, birth date, Social Security number, and financial account information. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
 Article Title: M&E Tax and Financial Services
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295172.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-05	CHROME Federal Credit Union	PA	3/6/2018	Electronic	Banking/Credit/Financial	Yes - Published #	3,122

We became concerned that two former employees may have downloaded files containing members' information prior to the end of their employment with CHROME. CHROME determined that the information the former employees may have had access to includes the names, addresses, dates of birth, Social Security numbers and bank account numbers of Maryland residents. (Number of records exposed per NC AG's notification)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
 Article Title: CHROME Federal Credit Union
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295174.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-03	Securus	TX	5/16/2018	Electronic	Business	Yes - Unknown #	Unknown

A hacker has broken into the servers of Securus, a company that allows law enforcement to easily track nearly any phone across the country, and which a US Senator has exhorted federal authorities to investigate. A spreadsheet allegedly from a database marked "police" includes over 2,800 usernames, email addresses, phone numbers, and hashed passwords and security questions of Securus users, stretching from 2011 up to this year.

Attribution 1 Publication: motherboard.vice.com Author:
 Article Title: Hacker Breaches Securus, the Company That Helps Cops Track Phones Across the US
 Article URL: https://motherboard.vice.com/en_us/article/gykgv9/securus-phone-tracking-company-hacked

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180518-01	US Marine Corps	DC	5/16/2018	Electronic	Government/Military	Yes - Published #	164,000

On Sept. 22, an airman with Okinawa's Joint Service Vehicle Registration Office at Camp Foster handed the disk to an Air Force security officer from Kadena Air Base. That security officer was tasked with bringing the disk — which was not password protected or encrypted — to Kadena security forces' headquarters, where the data were to be uploaded into the Air Force system. The disk was never seen again. It contained names, Social Security numbers, driver's license information, ID numbers, physical descriptions of personnel, vehicle identification numbers and plate numbers, service branch and duty information for servicemembers, dependents, civilian federal employees, contractors and local national master labor contractors.

Attribution 1 Publication: stripes.com Author:
 Article Title: Marines make changes after data of 164,000 people lost on Okinawa
 Article URL: <https://www.stripes.com/news/marines-make-changes-after-data-of-164-000-people-lost-on-okinawa-1.527438>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180517-09	Draper and Kramer, Inc.	IL	3/8/2018	Electronic	Business	Yes - Published #	3,000

At this time, we believe the incident may have resulted in the unauthorized access to the personal information. The personal information that may have been accessed in electronic form includes: name, Social Security number, driver's license number, passport number, account information and credit/debit card information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Draper and Kramer, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295202.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180517-08	Anchor Fund, LLC	CA	3/9/2018	Electronic	Banking/Credit/Financial	Yes - Published #	485

On February 7, 2018, an Anchor employee was preparing to send to a counterparty (via e-mail) routine reports containing information regarding disbursements and reinvestments for accounts invested in Anchor, including certain clients' names, addresses, Social Security numbers and account numbers. (Number of records exposed per NC AG's notification)

Attribution 1 Publication: MD AG's office Author:
Article Title: Anchor Fund, LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295206.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180517-07	Academy Mortgage Corporation (Workday)	UT	3/9/2018	Electronic	Banking/Credit/Financial	Yes - Published #	268

On January 24, 2018, Academy learned that direct deposit bank account information for a limited number of employees was changed within Workday, Academy's payroll application. Only direct deposit account information appeared to have been accessed by the unauthorized individual. However, Workday contains the Social Security numbers of employees, and may contain the names and Social Security numbers of any beneficiaries or dependents of the employee. (Number of records exposed per NC AG's notification)

Attribution 1 Publication: MD AG's office Author:
Article Title: Academy Mortgage Corporation
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295205.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180517-06	OrthoWest, Ltd.	OH	5/14/2018	Electronic	Medical/Healthcare	Yes - Published #	2,300

OrthoWest, Ltd. OH Healthcare Provider 2300 05/14/2018 Unauthorized Access/Disclosure Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: OrthoWest, Ltd.
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
ITRC20180517-05	Nova Southeastern University	FL	3/9/2018	Electronic	Educational	Yes - Published #	152

On February 9, 2018, we learned that an employee responded to a phishing email, believing it to be legitimate, which allowed an unauthorized actor to access the employee's email account. Our investigation determined that some of your information was contained in the affected email account and may have included your name, Social Security number, date of birth, and in some cases passport number. (Number of Records exposed per NC AG's office)

Attribution 1 Publication: MD AG's office Author:
Article Title: Nova Southeastern University
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295204.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180517-04	Southpoint Financial Services	GA	3/12/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On January 31, 2018, that forensic analysis was completed and the investigator notified us that a small number of Southpoint email inboxes had been compromised. These email accounts contained information that may have included your name, address, Social Security number, driver's license number and bank account information.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Southpoint Financial Services
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295213.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180517-03	Cambridge Dental Consulting Group	NV	5/11/2018	Electronic	Medical/Healthcare	Yes - Published #	3,758

Cambridge Dental Consulting Group (CDCG), a Las Vegas based provider of management and billing services for affiliated dental groups1 and other entities, notified approximately 3,750 patients of accidental exposure of personal health information and limited exposure of personally identifiable information after discovering a website malfunction. Even though the social security numbers of less than 3% of patients were accidentally exposed, CDCG is offering credit monitoring, upon request by affected patients.

Attribution 1 Publication: www.news3lv.com / hhs.gov Author:
Article Title: Local dental group notifies patients of data breach
Article URL: <http://news3lv.com/features/links/local-dental-group-notifies-patients-of-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180517-02	Davis Clinic / University of Texas Health Science Center	TX	5/16/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A clinic owned by the physicians organization of the University of Texas Health Science Center at Houston improperly sent out mass emails containing the email addresses of many of its patients.

Attribution 1 Publication: www.chron.com Author:
Article Title: UT physician group improperly shared patient email addresses
Article URL: <https://www.chron.com/news/medical/article/Patient-email-addresses-improperly-shared-by-UT-12917516.php>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180517-01	LifeBridge Health / LifeBridge Potomac Professionals	MD	5/16/2018	Electronic	Medical/Healthcare	Yes - Published #	538,127

On March 18, 2018, LifeBridge Health discovered that malware infected the server that host LifeBridge Potomac Professional's electronic medical record, and LifeBridge Health's patient registration and billing systems. The information potentially accessed may include patients' names, addresses, dates of birth, diagnoses, medications, clinical and treatment information, insurance information, and in some instances social security numbers.

Attribution 1 Publication: Company press release / CA AG's office Author:
Article Title: LifeBridge Health and LifeBridge Potomac Professionals Notify Patients of a Recent Security Incident
Article URL: <https://www.prnewswire.com/news-releases/lifebridge-health-and-lifebridge-potomac-professionals-notify-patients-of->

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-16	Atwood & Moore	TN	3/12/2018	Electronic	Business	Yes - Unknown #	Unknown

On October 28, 2017, we learned that the email account of an employee of Atwood and Moore was accessed by an unauthorized user. The information that was available in the potentially compromised email account included your name, and may also include your driver's license number, bank account number, and/or credit card number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Atwood & Moore
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295380.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-15	Rotary International	IL	3/13/2018	Electronic	Business	Yes - Published #	1,775

Working with third-party forensic investigators to confirm the nature and scope of the incident, on January 23, 2018, Rotary learned that several employee email accounts were subject to unauthorized logins by an unknown actor beginning in June 2017. The review of the accessible emails determined that the following types of information related to you may have been contained in the accessible emails: name, Social Security number, financial account / routing number, passport number, tax identification number, driver's license number, username/password, and medical/health insurance information. (Exposure number per IN AG's Office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
 Article Title: Rotary International
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295266.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-14	SallieMae	DE	3/13/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On «CALL_DT», a former employee may have obtained and shared the following information about you without authorization: name, address, social security number, date of birth and loan account information.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
 Article Title: SallieMae
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295218.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-13	UMH Properties, Inc.	NJ	3/15/2018	Electronic	Business	Yes - Published #	581

On February 23, 2018, we learned that one of our employees inadvertently emailed all of our employees' 2017 IRS Form W-2s to a current and a former employee. The information contained on your W-2 includes your name, address, earnings information, and Social Security number. (Exposure number per IN AG's Office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
 Article Title: UMH Properties, Inc.
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295270.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-12	Triage Consulting Group	CA	3/16/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 1, 2018, 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 our current and former employees. The information that was received by the unauthorized third party was W-2 information which included your full name, Social Security number, home address, 2017 compensation, and tax withholding information.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Triage Consulting Group
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295276.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-11	Presti & Naegele (CCH Client Access)	NY	3/19/2018	Electronic	Business	Yes - Published #	2,079

On February 14, 2018, Presti & Naegele became aware that it had fallen victim to a cyber intrusion by which an unknown party was able to access the firm's third-party vendor CCH Client Access Portal and some of its clients' personal information. Based on our investigation into this matter, we have determined that the personal information which may have been accessed includes first and last names, home addresses, Social Security numbers, and 2015, 2016 and/or 2017 tax return information, including compensation data. (Exposure number per IN AG's Office)

Attribution 1 Publication: MD AG's office Author:
 Article Title: Presti & Naegele (CCH Client Access)
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295281.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-10	Connexus Credit Union	MN	3/20/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

As a result, I am writing to inform you that Connexus was recently the target of an email phishing incident resulting in unauthorized access to three (3) employee email accounts. The personal information included your full name, Social Security number, driver's license number, and financial account number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Connexus Credit Union
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295379.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-09	Fireman Hospitality Group	NY	3/16/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 5, 2018, we learned that one of our HR employees received a phishing email designed to appear as if it came from one of our executives. Our ongoing investigation has determined that the unauthorized individual may have acquired your IRS Form W-2, which includes your name, address, earnings information, and Social Security number.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Fireman Hospitality Group
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295274.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-08	Hurst & Langlinais Ltd.	LA	3/21/2018	Electronic	Business	Yes - Published #	2,113

On March 8, 2018, the specialized forensic IT firm determined that there was unauthorized access to our system from a foreign IP address. The information may have included your: full name, birthdate, telephone number, address, Social Security number, all employment (W-2) and self-employment information, 1099 information, entity identification and income earned/amounts received from participation in S-Corp/partnership/LLC/trust, and direct deposit bank account information if provided to us (which includes account number and routing information). (Number of Records exposed per NC AG's office)

Attribution 1 Publication: MD AG's office Author:
Article Title: Hurst & Langlinais Ltd.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295292.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-05	Ross, Langan & McKendree, LLP	VA	3/27/2018	Electronic	Business	Yes - Unknown #	Unknown

On February 26, 2018, RLM learned that unauthorized emails had been sent from some employee email accounts. (Type of information per MD AG's notification)

Attribution 1 Publication: MD AG's office Author:
Article Title: Ross, Langan & McKendree, LLP
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295006.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-04	Pro World	NJ	3/27/2018	Electronic	Business	Yes - Unknown #	Unknown

On February 25, 2018, we identified unauthorized computer code added to the checkout page of our online store at <https://www.proworldinc.com>. The information on the checkout page that the code potentially captured includes name, address, phone number, email address, payment card number, expiration date, and card security code (CVV).

Attribution 1 Publication: MD AG's office Author:
Article Title: Pro World
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295005.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-02	MedEvolve	AR	5/16/2018	Electronic	Medical/Healthcare	Yes - Published #	205,000

More than 200,000 patients' records were exposed on MedEvolve's public FTP server. One of the two clients where no password or protection was deployed was Premier Urgent Care in Exton, Pennsylvania. More than 11,000 of the records reportedly included Social Security numbers. A second MedEvolve client with exposed patient information was Dr. Beverly Held, a dermatologist in Corpus Christi, Texas. The researcher estimated that there were about 12,000 Social Security numbers exposed in the files.

Attribution 1 Publication: databreaches.net Author:
 Article Title: More than 200,000 patients' records were exposed on MedEvolve's public FTP server – researcher
 Article URL: <https://www.databreaches.net/more-than-200000-patients-records-were-exposed-on-medevolves-public-ftp-server-rese>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180516-01	Baptist Health	AR	5/7/2018	Electronic	Medical/Healthcare	Yes - Published #	3,453

Baptist Health AR Healthcare Provider 3453 05/07/2018 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
 Article Title: Baptist 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
ITRC20180515-01	Medical Center Ophthalmology	TX	4/30/2018	Electronic	Medical/Healthcare	Yes - Published #	3,017

Medical Center Ophthalmology Associates TX Healthcare Provider 3017 04/30/2018 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: Medical Center Ophthalmology
 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
ITRC20180514-15	Technical Needs North, Inc.	NH	4/19/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 6, 2018, Tech Needs discovered that it had inadvertently misaddressed the IRS Form 1095-C Affordable Care Act health coverage confirmation forms to other employees. As a result of its investigation, it learned that personal information, which included names and Social Security numbers, may have been disclosed.

Attribution 1 Publication: NH AG's office Author:
 Article Title: Technical Needs North, Inc.
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/technical-needs-20180419.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-14	Julian Sur, CPA	PA	4/26/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 28, 2018, I learned that there was potentially unauthorized access from a foreign IP system to my e-mails from approximately February 9-26, 2018. If I prepared tax returns for you, the information may have included all information provided to the taxing authorities including your: full name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information (if provided), all 1099 information (including account number if provided), driver's license information (if provided), and direct deposit bank account information (including account number and routing information if provided).

Attribution 1 Publication: MD AG's office Author:
 Article Title: Julian Sur, CPA
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-297364.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-13	McMahan, Thomson & Associates, PC (CPAs)	MI	4/27/2018	Electronic	Business	Yes - Published #	2,677

We recently learned that our computer system may be infected with malware. An extensive manual document review, which concluded on March 27, 2018, confirmed that your information that was contained in the files that were potentially accessed included your name, address, and Social Security number, and may have included your driver's license number. (Exposure number per IN AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: McMahan, Thomson & Associates, PC (CPAs)
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/mcmahan-20180427.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-12	Malley's Chocolates	OH	5/10/2018	Electronic	Business	Yes - Published #	3,453

A computer hacker hit Malley's Chocolates two weeks before Easter and stole credit and debit card information belonging to 3,453 customers.

Attribution 1 Publication: cleveland.com / NH AG's office / MT AG' Author:
Article Title: Malley's Chocolates' website hacked, 3,400 online customers' card information breached
Article URL: http://www.cleveland.com/business/index.ssf/2018/05/malleys_chocolates_website_hac.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-11	Fredericksburg School System	VA	5/8/2018	Electronic	Educational	Yes - Unknown #	Unknown

Hackers phishing for sensitive information faked an email from a regional organization to break into the Fredericksburg school system's electronic mail and file system last month. This could give the intruders access to such information as a student's name, address, date of birth and grade, as well as a parent's or guardian's name, phone number, email address and insurance information.

Attribution 1 Publication: fredericksburg.com Author:
Article Title: Hackers break into Fredericksburg school system's emails, file
Article URL: <http://www.fredericksburg.com/news/local/fredericksburg/hackers-break-into-fredericksburg-school-system-s-emails-f>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-10	Baystate Family Dental, Inc.	MA	5/4/2018	Paper Data	Medical/Healthcare	Yes - Published #	500

Baystate family dental inc MA Healthcare Provider 500 05/04/2018 Theft Desktop Computer, Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Baystate Family Dental, 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
ITRC20180514-09	DigiPen Institute of Technology	WA	5/7/2018	Electronic	Educational	Yes - Unknown #	Unknown

On April 25, 2018, an authorized DigiPen employee inadvertently emailed a spreadsheet containing certain students' personal information to a recipient that was not authorized to access that information (as opposed to the email's intended recipient). The spreadsheet included each student's full name, Social Security numbers, student ID, and the program in which the student was enrolled.

Attribution 1 Publication: NH AG's office / MT AG's office Author:
Article Title: DigiPen Institute of Technology
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/digipen-20180507.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-08	LaPorte & Associates, Inc.	OR	5/11/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 9, 2018, LaPorte learned that a laptop belonging to one of its agents was stolen. The data potentially subject to unauthorized access varies, but includes some combination of the individual's name, mailing address, Social Security numbers, driver's license numbers, health insurance numbers, claims information, dates of service, provider names, diagnoses or treatment information, and explanations of benefits, invoice amounts, and invoices.

Attribution 1 Publication: Company notice / NH AG's office Author:
Article Title: LaPorte & Associates, Inc.
Article URL: <https://www.prnewswire.com/news-releases/laporte-notifies-individuals-of-security-incident-300647155.html>



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

Report Date: 7/2/2018

Page 49 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-07	Cerebral Palsy Research Foundation of Kansas	KS	5/14/2018	Electronic	Medical/Healthcare	Yes - Published #	8,300

The investigation into the breach determined that while the database had been created on a secure subdomain in early 2000, when CPRF switched its servers in 2017 the database was not identified resulting in the accidental removal of security protections. The breach was limited to personal information and personal health information relating to the type of disability suffered by patients.

Attribution 1 Publication: [hipaajournal.com / hhs.com](#) Author:

Article Title: 8,300 Cerebral Palsy Research Foundation of Kansas Patients Informed of 10-Month Exposure of PHI

Article URL: <https://www.hipaajournal.com/8300-cerebral-palsy-research-foundation-of-kansas-patients-informed-of-10-month-expo>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-06	Mason Law Office, P.C.	CA	5/5/2018	Electronic	Business	Yes - Unknown #	Unknown

Client data was potentially accessed, client case information was deleted, and other administrative changes were made to the system. Information potentially accessed includes client names, social security numbers, driver's license numbers, phone numbers, email addresses, as well as legally privileged/protected information, including legal documents, case notes, disclosures, financial statements, evidence, photos, invoices, transcripts, trust balances, and attorney-client communications.

Attribution 1 Publication: CA AG's office Author:

Article Title: Mason Law Office, P.C.

Article URL: https://oag.ca.gov/system/files/NOTICE%20TO%20CLS%20RE%20MYCASE%20DATA%20BREACH_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-05	Deephaven Mortgage LLC	NC	5/8/2018	Electronic	Banking/Credit/Financial	Yes - Published #	5,593

Our investigation revealed that Deephaven Mortgage was the victim of an email phishing attack resulting in unauthorized access to and acquisition of the contents of certain employee email accounts. Our investigation determined that the information present in the affected email accounts contained some of your personal information, including one or more of the following identity-related items: name, address, date of birth and Social Security number.

Attribution 1 Publication: CA AG's office / MT AG's office Author:

Article Title: Deephaven Mortgage LLC

Article URL: https://oag.ca.gov/system/files/Deephavensample%20050818_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-04	Farmgirl Flowers	CA	5/11/2018	Electronic	Business	Yes - Published #	1,870

The unauthorized access involved the insertion of rogue code into our checkout page. The information that was accessed without authorization could have included your name, billing address for a credit card, telephone number, email address, and credit card information including card number, name on card, issuer, expiration date, and security code. (Exposure number per IN AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office Author:

Article Title: Farmgirl Flowers

Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/farmgirl-flowers-20180509.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-03	Chili's Grill and Bar / Brinker International	TX	5/12/2018	Electronic	Business	Yes - Unknown #	Unknown

On May 11, 2018, we learned that some of our Guests' payment card information was compromised at certain Chili's restaurants as the result of a data incident. Based on the details of the issue currently uncovered, we believe that malware was used to gather payment card information including credit or debit card numbers as well as cardholder names from our payment-related systems for in-restaurant purchases at certain Chili's restaurants.

Attribution 1 Publication: Chili's notification Author:

Article Title: Chili's Grill and Bar

Article URL: <http://brinker.mediaroom.com/ChilisDataIncident>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-02	Capital Administrators, Inc.	CA	5/11/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 30, Capitol learned through a forensic investigation of a phishing email incident that certain emails and attachments had been accessed by an unauthorized person. Type of information exposed was not disclosed.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Capital Administrators, Inc.
 Article URL: https://oag.ca.gov/system/files/Sample_Capitol_Individual_Notice_Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180514-01	Nuance Communications (multiple entities)	MA	5/11/2018	Electronic	Business	Yes - Published #	45,000

Nuance Communications, which specializes in speech recognition software, says an unauthorized third party accessed one of its medical transcription platforms, exposing 45,000 individuals' records. Exposed data included names, birth dates, medical record and patient numbers, as well as service details such as patient conditions, assessments, treatments, care plans and dates of service.

Attribution 1 Publication: Bankinfosecurity.com / hipaajournal.com Author:
 Article Title: Nuance Communications Breach Affected 45,000 Patients
 Article URL: <https://www.bankinfosecurity.com/nuance-communications-breach-affected-45000-patients-a-11002>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180510-02	Tigervision, LLC dba Eye Care Surgery Center, Inc.	LA	4/27/2018	Electronic	Medical/Healthcare	Yes - Published #	2,553

On February 26, 2018, we discovered that a laptop computer was stolen. Although we are not aware of the misuse of any information, we could not rule out the possibility that your personal information, including your name, date of birth, and diagnosis information may be at risk.

Attribution 1 Publication: Company website Author:
 Article Title: Tigervision, LLC dba Eye Care Surgery Center, Inc.
 Article URL: <https://www.eyecaresurgerycenterbr.com/wp-content/uploads/2018/04/Substitute-Notice-ECSC.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180510-01	US Acute Care Solutions (USACS)	OH	5/8/2018	Electronic	Medical/Healthcare	Yes - Published #	15,552

The investigation determined that the unauthorized third party illegally gained access to one USACS email account containing patient information. The email account may have included some of your information, including your name, address, date of service USACS account number, medical and health insurance information, diagnostic and treatment information, and Social Security number.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
 Article Title: US Acute Care Solutions (USACS)
 Article URL: https://oag.ca.gov/system/files/letter_USACS_May%202018_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-13	Wealth Management, Inc.	AR	3/28/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On February 23, 2018, Wealth Management learned that an unauthorized individual gained access to an employee's email account which contained messages with individuals' personal information. Based on this investigation, it was determined that some personal information was accessed, including possibly names, addresses, dates of birth, Social Security numbers, driver's license numbers, and account numbers.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Wealth Management, Inc.
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295355.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-12	Morgenthaler Private Equity	OH	3/28/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

In late February, we learned of an incident that occurred on January 19, 2018, that resulted in unauthorized access to data files within our system. Unfortunately, we believe the unauthorized user may have obtained access to certain personal information, including your name, address, email address, social security number, and financial account information.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Morgenthaler Private Equity
 Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295346%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295346%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-11	Franklin American Mortgage Company	TN	3/28/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We were made aware that certain e-mail correspondence between FAMC and others involved in the origination process of your loan was sent to a non-FAMC e-mail address during the period described above without FAMC's knowledge. This incident involved certain personal non-public information that may have included your name, address, complete or partial account numbers, Social Security Number, birth date, phone number, driver license information, e-mail address, employment information, and/or other identifying information.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Franklin American Mortgage Company
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295340.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-10	Lincoln National Life Insurance Company	IN	3/29/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Lincoln recently discovered that one of its employees was the victim of a phishing attack which resulted in a third party gaining limited unauthorized access to the employee's account for a period of time between Jan. 29 and Jan. 31, 2018. Based on the facts known to Lincoln at this time, the personal information affected by this unauthorized access may have included a combination of your name, address, date of birth, claim number, Social Security number and/or health information.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Lincoln National Life Insurance Company (1/29/18)
 Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295367%20\(1\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295367%20(1).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-09	Tidewater Mortgage Services, Inc.	VA	3/30/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On February 7, 2018, during the course of investigating phishing e-mails sent to their employees, TMSI learned that an unauthorized individual gained access to certain TMSI employees' e-mail accounts that may have contained personal information. TMSI conducted a thorough review of the affected e-mail accounts and determined that an e-mail or an attachment to an e-mail in one of the accounts contained the names, driver's license numbers, Social Security numbers, bank account numbers, and routing numbers of a Maryland resident.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Tidewater Mortgage Services, Inc.
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295373.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-08	Mattress Firm, Inc.	TX	1/3/2018	Electronic	Business	Yes - Published #	Unknown

On November 9, 2017, a "phishing" e-mail was sent to users on the Mattress Firm e-mail domain which contained a link to a third-party website. The Company believes that an unknown party then used these harvested credentials to gain access to the compromised users' accounts on our HR Information System, where personal information (e.g., name, social security number and bank account number) is viewable.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
 Article Title: Mattress Firm
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294949.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-07	Alabama Ballet	AL	3/30/2018	Electronic	Business	Yes - Unknown #	Unknown

The Alabama Ballet was the victim of a ransomware attack that likely occurred during the late night hours of Friday, March 2, 2018. Our IT professional concluded his investigation on March 13, 2018, which revealed that your personal information may have been exfiltrated, including your full name, social security number, and direct deposit information (if you were paid by the Ballet through a direct deposit system as opposed to payment by check).

Attribution 1 Publication: MD AG's office Author:
 Article Title: Alabama Ballet
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295372.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-06	Securadyne Systems LLC	TX	1/16/2018	Electronic	Business	Yes - Unknown #	Unknown

On or about September 12, 2017, we discovered that Securadyne Systems LLC ("Securadyne") had become the target of a phishing email campaign and that several employees had clicked on the phishing email and entered their credentials. Type of information exposed was not disclosed.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Securadyne Systems LLC
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294957.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-05	Anchorage School District	AK	1/17/2018	Electronic	Educational	Yes - Published #	865

On December 7, 2017, ASD learned that an unauthorized individual utilized a phishing scheme to gain access to an ASD employee's email account on the same day. (Number of records exposed and type of exposed information per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
 Article Title: HSBC Mortgage Services, Inc.
 Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294955%20\(1\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294955%20(1).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-03	Global University	MS	5/8/2018	Electronic	Educational	Yes - Published #	139,810

Through this investigation, Global determined on February 23, 2018, that a database containing information related to current and former Global students was misconfigured and accessible to the Internet from December 31, 2017 to January 31, 2018. The investigation determined the misconfigured database contained personal information including names, Social Security numbers, and for a limited number of individuals, date of birth. (Exposure number per IN AG's Office)

Attribution 1 Publication: Company website / CA AG's office / VT Author:
 Article Title: Global University Provides Notice Of Data Breach
 Article URL: <https://www.prnewswire.com/news-releases/global-university-provides-notice-of-data-breach-300644987.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-02	Oregon Clinic	OR	5/9/2018	Electronic	Medical/Healthcare	Yes - Published #	64,487

On March 9, 2018, The Oregon Clinic learned that an unauthorized third party accessed an email account. The following information may have been affected: names, dates of birth, and certain medical information. This medical information may include medical record numbers, diagnosis information, medical condition, diagnostic tests performed, prescription information, and/or health insurance information. For a small subset of patients, Social Security numbers may also have been affected.

Attribution 1 Publication: Company website / hhs.gov / MT AG's of Author:
 Article Title: Oregon Clinic
 Article URL: <http://www.oregonclinic.com/dataincident>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180509-01	Knoxville Heart Group, LLC	TN	4/27/2018	Electronic	Medical/Healthcare	Yes - Published #	15,995

Knoxville Heart Group, Inc. TN Healthcare Provider 15995 04/27/2018 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: Knoxville Heart Group, 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
ITRC20180508-15	Hanover Insurance Company	MA	3/27/2018	Electronic	Business	Yes - Published #	13,600

Upon learning of suspicious activity, we immediately took steps to block any further unauthorized access, commenced an investigation, and engaged a leading information security and forensics firm to assist. Subsequently, The Hanover undertook a comprehensive review of the emails in the service accounts and determined on February 26, 2018 that an email, or attachment, contained certain information about some of its Maryland customers, which may have included names, addresses, Social Security numbers, and/or driver's license numbers.

Attribution 1 Publication: MD AG's office / IN AG's office / NC AG' Author:
 Article Title: Hanover Insurance Company
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295007.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-14	Vidant Medical Group LLC	NC	3/27/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

The vehicle of an employee of Vidant General Surgery - Edenton was broken into sometime during the night between January 2 and January 3, 2018. The stolen records may have included the following information: your name, address, date of birth, full Social Security number, medical record number, medications, problem list, primary care provider's name, physician progress notes, diagnosis, pathology report, operative report, and other treatment information.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Vidant Medical Group LLC
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295000.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-13	Southwest Airlines Co.	TX	3/29/2018	Electronic	Business	Yes - Published #	36,485

On March 2, 2018, we learned that an unauthorized third party modified a limited number of Employees' direct deposit information on their respective SWALife accounts. In addition to your deposit account and routing numbers, the unauthorized party had the ability to access other information in your SWALife account, which may have included your name, address, phone number, email address, employee identification number, date of birth, Social Security number, passport information, wage and payroll information, insurance and other benefits information, and your W-2 and 1095-C tax forms. (Exposure number per IN AG's office)

Attribution 1 Publication: MD AG's office Author:
 Article Title: Southwest Airlines Co.
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295371.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-12	Rx Valet LLC	GA	5/4/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Some time in late 2017, a database containing the Company's customer order records (the "Database") became publicly exposed to the internet as a result of a server misconfiguration. The data exposed and accessed included personal information such as name, email address, physical address, and order information including (1) items ordered, including medication name and (2) obscured credit card numbers (in which only the last four digits of the card number were readable).

Attribution 1 Publication: NH AG's office Author:
 Article Title: Rx Valet LLC
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/rx-valet-20180504.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-11	Pioneer Bankcorp, Inc. dba First Bank	FL	5/1/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On April 9, 2018, we learned that certain of your personal information could have been viewed as part of an email account compromise. You are receiving this notice because certain of your personal information was in the account and could have been accessed, including your name, address Social Security number and driver's license number.

Attribution 1 Publication: NH AG's office Author:
 Article Title: Pioneer Bankcorp, Inc. dba First Bank
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/pioneer-bankcorp-20180501.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-10	Florida Agency for Persons with Disabilities (FAPD)	FL	3/1/2018	Electronic	Government/Military	Yes - Published #	63,627

In February, a more extensive phishing attack occurred that resulted in multiple email accounts being compromised. That phishing attack affected more than 55,000 customers, whose names, birth dates, and Social Security numbers were potentially compromised.

Attribution 1 Publication: hhs.gov Author:
 Article Title: Florida Agency for Persons with Disabilities
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Attribution 2 Publication: hipaajournal.com / hhs.gov Author:
 Article Title: Florida Agency for Persons with Disabilities (FAPD)
 Article URL: <https://www.hipaajournal.com/florida-agency-for-persons-with-disabilities-and-black-river-medical-center-report-phish>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-09	Walmart, Inc.	AR	3/26/2018	Electronic	Medical/Healthcare	Yes - Published #	741

Walmart Inc. AR Healthcare Provider 741 03/26/2018 Unauthorized Access/Disclosure Email, Other

Attribution 1 Publication: hhs.gov Author:
 Article Title: Walmart, 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
ITRC20180508-08	Walgreen Company	IL	4/6/2018	Electronic	Medical/Healthcare	Yes - Published #	910

Walgreen Co. IL Healthcare Provider 910 04/06/2018 Theft Other

Attribution 1 Publication: hhs.gov Author:
 Article Title: Walgreen 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
ITRC20180508-07	Walgreen Company	IL	4/27/2018	Paper Data	Medical/Healthcare	Yes - Published #	1,692

Walgreen Co. IL Healthcare Provider 703 04/27/2018 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: Walgreen 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
ITRC20180508-06	CashNetUSA	IL	4/27/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Beginning on or about March 23, 2018, our security team discovered that an unauthorized party used valid email addresses and passwords to log in to a small percentage of CashNetUSA accounts. Access to an account could have enabled the unauthorized party to view the account holder's name, telephone number, physical address, email address, their bank account number, CashNetUSA Customer ID and Loan ID, last four digits of their Social Security number, last four digits of their driver license, and basic employment and income information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-05	Children's Mercy Hospital	KS	4/30/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On Dec. 2, 2017, the Children's Mercy Information Security team detected unauthorized account access to two employee email accounts associated with a phishing email. The categories of information vary for individuals, but may have included first and last name, medical record number, gender, date of birth, age, height, weight, body mass index, admission date, discharge date, procedure date, diagnostic and procedure codes, clinical information, demographic information, diagnosis, conditions, other treatment information and identifying or contact information.

Attribution 1 Publication: Hospital website / CA AG's office / MT A Author:
Article Title: Children's Mercy Hospital
Article URL: <https://www.childrensmercy.org/February2018/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-04	Building Profits LLC	NV	4/30/2018	Electronic	Business	Yes - Unknown #	Unknown

On or about October 19, 2017, Building Profits, LLC ("Building Profits") became aware of unusual activity on an employee laptop. Certain data pertaining to Building Profits clients was accessible on the impacted computer during the periods of unusual activity. Type of information exposed was not disclosed.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-03	Blattner Energy, Inc.	MN	4/30/2018	Electronic	Business	Yes - Published #	248

On February 9, 2018, Blattner learned of a potential data security incident that may have affected personal information contained within an employee's email account. The following personal information may have been involved in this incident – <<ClientDef1(name, address, Social Security number, date of birth, driver's license or other government identification number, and/or medical information.)>> (Exposure number per IN AG's Office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-02	SA Stone Wealth Management	GA	4/30/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On or about February 28, 2018, it came to my attention that my e-mail had been hacked. That information may include the types of information normally found on account opening documents and letters of authorization, such as your name, address, birthdate, telephone number, account number, e-mail address, and social security number.

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



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180508-01	Bennett Thrasher LLP	GA	4/30/2018	Electronic	Business	Yes - Unknown #	Unknown

On April 6, 2018, the Firm became aware that an unauthorized third party accessed a portal hosted by Commerce Clearing House (CCH). The information contained in the documents maintained in the CCH portal included your first and last name, address, Social Security number ("SSN") and, in certain circumstances, medical/health insurance information and/or bank/brokerage account information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180507-07	Walker Advertising, LLC	CA	4/9/2018	Electronic	Business	Yes - Unknown #	Unknown

Two senior Walker employees' corporate e-mail accounts were hacked between approximately January 29, 2018 and February 22, 2018. The IT Department's investigation determined that potentially accessed information in the corporate e-mail accounts may include your name, Social Security number, driver's license number, medical information, and health insurance information.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Walker Advertising, LLC
 Article URL: <https://oag.ca.gov/system/files/Individual%20Notification%20California-%20Experian%20%28Client%20Approved%29>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180507-06	WithumSmith+Brown, PC	NJ	4/25/2018	Electronic	Business	Yes - Published #	228

On April 10, 2018, we became aware that an unknown, unauthorized third party gained access to an employee's email account as the result of a phishing attack. The investigation determined that an email with an attachment that included your name, address, and Social Security number may have been compromised. (Exposure number per IN AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: WithumSmith+Brown
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/withumsmith-20180425.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180507-05	Sekisui Diagnostics	MA	4/26/2018	Electronic	Medical/Healthcare	Yes - Published #	194

On Friday, April 6, 2018 while intending to send a W2 to a former employee, a file containing the W2s of all US employees was inadvertently attached to the email. The email contained your W2 which included your name, address, social security number and 2017 wages, taxes and withholdings. (Exposure number per IN AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: Sekisui Diagnostics
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/sekisui-20180426.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180507-04	Rail Europe North America	DE	4/24/2018	Electronic	Business	Yes - Published #	18,785

Upon discovery that this malicious intrusion may have compromised users' personal information, we immediately cut off from the Internet all compromised servers on February 16, 2018, and engaged information security experts to assist with forensic analysis, system restoration and security hardening. The personal information that may have been involved is: name, gender, delivery address, invoicing address, telephone number, email address, credit/debit card number, expiration date and CVV of customers, and, in some cases, username and password of registered users who created personal accounts on a RENA website. (Exposure number per IN AG's Office)

Attribution 1 Publication: CA AG's office / VT AG's office Author:
 Article Title: Rail Europe North America
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/rail-europe-20180424.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180507-03	Athens Heart Center, PC	GA	4/16/2018	Electronic	Medical/Healthcare	Yes - Published #	12,158

Athens Heart Center, P.C. GA Healthcare Provider 12158 04/16/2018 Hacking/IT Incident Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
 Article Title: Athens Heart Center, 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
ITRC20180507-02	Rutland Regional Medical Center	VT	4/26/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On or about February 22, 2018, Rutland Regional Medical Center ("RRMC") discovered that log-in credentials belonging to certain employees' GreenShades accounts were compromised. Through its ongoing forensic investigation of the incident, RRMC learned your GreenShades account may have been accessed by an unauthorized person. Our investigation determined the information present in the GreenShades account included your paystubs; W2s; Social Security number; date of birth; address; home phone number; gender and marital status.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Rutland Regional Medical Center
 Article URL: <http://ago.vermont.gov/blog/category/security-breaches/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180507-01	National Restaurant Association	DC	4/30/2018	Electronic	Business	Yes - Unknown #	Unknown

Through this investigation, we learned on or around November 28, 2017, that several employee email accounts were subject to unauthorized logins by an unknown actor. Type of information exposed was not disclosed.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180504-04	CPT Group, Inc.	CA	4/27/2018	Electronic	Business	Yes - Published #	42,587

On February 8, 2018, CPT learned through its ongoing forensics investigation of a phishing email incident that certain emails and attachments could have potentially been accessed by an unauthorized person. The information that could have been accessed in the affected employee's account includes your name, address, and Social Security number. (Exposure number per IN AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / VT AG' Author:
 Article Title: CPT Group, Inc.
 Article URL: https://oag.ca.gov/system/files/CPT_CA_NotificationFinal_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180504-03	Cetera Advisors LLC (4/26)	CO	4/26/2018	Electronic	Business	Yes - Published #	2,299

On or about February 9, 2018, Cetera learned that an unauthorized individual gained access to some of your personal information. As part of the investigation, it was determined that some personal information was accessed, including possibly your name, address, date of birth, Social Security number, driver's license number, and/or your account number. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office / VT AG's office Author:
 Article Title: Cetera Advisors LLC (4/26)
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/cetera-20180426.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180504-02	Educational Testing Service	NJ	1/25/2018	Electronic	Business	Yes - Unknown #	Unknown

On December 12, 2017, we discovered that credentials to an ETS email account used in connection with Praxis test takers (Account) may have been compromised. Subsequent to this discovery, we investigated the issue and discovered that the Account had been accessed by an unknown and potentially unauthorized user. Information involved included: the first and last names, social security numbers, and other personal information of some Praxis test-takers.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Educational Testing Service
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295025.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180504-01	Scenic Bluffs Community Health Centers	WI	5/4/2018	Electronic	Medical/Healthcare	Yes - Published #	2,889

An unauthorized individual has gained access to the email account of an employee of Scenic Bluffs Community Health Centers and potentially viewed the protected health information of up to 2,889 patients. While no PHI appeared to have been obtained by the attacker, it is possible that during the time that access to the email account was possible, PHI detailed in the emails could potentially have been viewed.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
 Article Title: 2,889 Patients of Scenic Bluffs Community Health Centers Notified of PHI Breach
 Article URL: <https://www.hipaajournal.com/2889-patients-of-scenic-bluffs-community-health-centers-notified-of-phi-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180503-05	Liberty Tax Service	VA	5/2/2018	Paper Data	Business	Yes - Unknown #	Unknown

An anonymous tip a few days ago directed 8 On Your Side consumer reporter Brian Roche to the dumpster behind a Liberty Tax Service office on Willow Street Pike that just closed last week. Among the items he found were folders with W-2 forms attached, tax documents and tax work sheets with personal information that included Social Security numbers and bank account numbers.

Attribution 1 Publication: wgal.com Author:
 Article Title: Personal information found in dumpster behind tax prep office in Lancaster County
 Article URL: <http://www.wgal.com/article/personal-information-found-in-dumpster-behind-tax-prep-office-in-lancaster-county/20127>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180503-04	Worldwide Insurance Services, LLC dba GeoBlue	PA	4/30/2018	Electronic	Medical/Healthcare	Yes - Published #	1,692

Following the conclusion of our investigation of a suspected security incident, with the assistance of a leading computer forensic firm, we determined that an unauthorized party obtained credentials to two employees' email accounts through a phishing email scheme. Other than PHI, any other type of information exposed was not disclosed.

Attribution 1 Publication: Company notice / hhs.gov Author:
 Article Title: Worldwide Insurance Services, LLC dba GeoBlue
 Article URL: https://oag.ca.gov/system/files/GeoBlue%20Adult%20CM_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180503-03	Florida Hospital	FL	5/3/2018	Electronic	Medical/Healthcare	Yes - Published #	12,724

Three websites used by Florida Hospital have been infected with malware that has potentially allowed the threat actors behind the attack to obtain patients' protected health information. Potentially, patients' names, birth dates, email addresses, phone numbers, insurance carriers, the last four digits of their social security numbers, any comments uploaded via the sites, and their height and weight have potentially been obtained by the attackers.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
 Article Title: Malware Installed on Florida Hospital Websites May Have Provided Access to PHI
 Article URL: <https://www.hipaajournal.com/malware-installed-on-florida-hospital-websites-may-have-provided-access-to-phi/>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180503-02	Maximus, Inc. (Business Ink)	VA	5/3/2018	Paper Data	Business	Yes - Published #	3,029

Maximus Inc, a provider of business process management and technology solutions to government health and human services agencies, is alerting more than 3,000 individuals that some of their protected health information has been accidentally disclosed to other individuals as a result of a printing error on a recent mailing. The types of information detailed on the page were limited to names, addresses, group numbers, case numbers, and program type.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
 Article Title: PHI of 3,000 Patients Exposed Due to Mailing Printing Error
 Article URL: <https://www.hipaajournal.com/phi-of-3000-patients-exposed-due-to-mailing-printing-error/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180503-01	Parker Staffing Services	WA	3/15/2018	Electronic	Business	Yes - Unknown #	Unknown

On February 15th, 2018 Parker Staffing Services, LLC learned that a PDF file containing W-2 statements had been inadvertently disclosed to an outside individual via email attachment.

Attribution 1 Publication: WA AG's office Author:
 Article Title: Parker Staffing Services
 Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/ParkerStaffingServi

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180502-01	Capital District Physicians' Health Plan	NY	4/20/2018	Paper Data	Medical/Healthcare	Yes - Published #	839

Capital District Physicians' Health Plan NY Health Plan 839 04/20/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: Capital District Physicians' 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
ITRC20180430-04	Billings Clinic Atrium Pharmacy	MT	4/27/2018	Electronic	Medical/Healthcare	Yes - Published #	949

Billings Clinic contacted 949 patients to let them know about a data security incident involving personal information in Billings Clinic's email system Friday. Information that was potentially viewed includes patient names, dates of birth, phone numbers and amounts owed to Billings Clinic's Atrium Pharmacy.

Attribution 1 Publication: ktvq.com / hhs.gov Author:
 Article Title: Billings Clinic notifies nearly 1,000 patients of data breach
 Article URL: <http://www.ktvq.com/story/38061421/billings-clinic-notifies-nearly-1000-patients-of-data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180430-03	Zippy's Restaurants	HI	4/28/2018	Electronic	Business	Yes - Unknown #	Unknown

Zippy's announced late this afternoon that it suffered a major security breach affecting customers at its Hawaii restaurants. Information compromised in the breach involved credit and debit cards, containing the name of the account holder, the account number, the verification code, and the card's expiration date.

Attribution 1 Publication: governor.hawaii.gov Author:
 Article Title: State Office of Consumer Protection Investigating Security Breach at Zippy's
 Article URL: <http://governor.hawaii.gov/newsroom/latest-news/state-office-of-consumer-protection-investigating-security-breach-at>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180430-02	Complete Family Medicine, LLC	NE	4/30/2018	Paper Data	Medical/Healthcare	Yes - Published #	1,331

Burglars broke into Complete Family Medicine, part of Great Plains Physician Network in North Platte, Neb., on March 1, taking a computer used to conduct EKGs and uncashed patient checks that were in a locked safe. While some checks were recovered, the computer, which held patient names, dates of birth and EKG images, remains missing. Patient information on missing checks includes names, addresses and bank account numbers.

Attribution 1 Publication: [healthdatamanagement.com / hhs.gov](http://healthdatamanagement.com/hhs.gov) Author:
 Article Title: Computer with patient info, checks stolen from Nebraska practice
 Article URL: <https://www.healthdatamanagement.com/news/computer-with-patient-info-checks-stolen-from-nebraska-practice>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180430-01	Buxbaum Daue PLLC	MT	4/11/2018	Electronic	Business	Yes - Unknown #	Unknown

On June 6, 2017, a Buxbaum Daue team member's rental vehicle was vandalized and burglarized near the San Francisco airport and several electronic devices were stolen, including a laptop. The information that was available in the stolen laptop would include file information that included your name, Social Security number, and may have also included health or medical information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-24	MCR Investors LLC	NY	4/23/2018	Electronic	Banking/Credit/Financial	Yes - Published #	6,178

On March 11, 2018, we learned that one of our employees had their password-protected laptop stolen. On April 9, 2018 the investigation concluded that the laptop contained some of your personal information. last four digits of their Social Security number, last four digits of their driver license (Exposure number per MA OCABR)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-23	Golter Law Office, LLC	AK	4/13/2018	Electronic	Business	Yes - Unknown #	Unknown

On October 31, 2017, we learned that a hard drive had been stolen from a Golter employee's vehicle. The information that was accessible in the hard drive included your name and Social Security number, and may have also included your driver's license number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-22	Visit Baltimore (ADP, LLC)	MD	1/31/2018	Electronic	Business	Yes - Unknown #	Unknown

On December 18, 2017, ADP unintentionally mailed hardcopy W-2 previews for Visit Baltimore's employees to the Human Resources department of a law firm client of ADP (the "Incident"). The data exposed by ADP to its law firm client included, among other things, the name, mailing address, Social Security Number, wage information and other information disclosed on the W-2s for Visit Baltimore's employees for their respective 2017 personal income tax years.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Visit Baltimore / ADP, LLC
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295036.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-21	Eagle Bancorp, Inc.	MD	1/31/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On January 9, 2018, someone broke into the car of an EagleBank employee and stole a company laptop. Upon learning of the incident, EagleBank determined that the laptop contained a small amount of customer information, including one Maryland resident's name, date of birth, Social Security number and driver's license number.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Eagle Bancorp, Inc.
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295008.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-20	Duquesne University	PA	1/31/2018	Electronic	Educational	Yes - Published #	196

On Friday, January 26, 2018, the Duquesne University School of Law, Office of Admissions, sent an email inviting prospective students to attend an upcoming meeting with our Associate Director of Admissions. A spreadsheet regarding some prospective students was inadvertently attached to the email. The information contained in the spreadsheet included your name, Social Security number, LSAT score, and other information relating to the admissions process. (Exposure number per NC AG's office)

Attribution 1 Publication: MD AG's office Author:
 Article Title: Duquesne University
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294966.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-19	Doral Corporation	WI	2/2/2018	Electronic	Business	Yes - Published #	335

Doral Corporation was the victim of an email spoofing attack on January 23, 2018, by an individual pretending to be Doral Corporation's President. Unfortunately, a PDF document containing the names, Social Security numbers and wage/salary information for all 2017 employees was provided before the company discovered that the request was made from a fraudulent account by someone using the name and email address that appeared to be from Doral Corporation's President. (Exposure number per IN AG's office)

Attribution 1 Publication: MD AG's office Author:
 Article Title: Doral Corporation
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294992.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-18	MidCap Financial Services	MD	2/5/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

In the third week of November 2017, an unknown attacker gained unauthorized access to the webmail account of a single MidCap employee. he potentially compromised personal information includes the names and Social Security numbers of the affected individuals.

Attribution 1 Publication: MD AG's office Author:
 Article Title: MidCap Financial Services
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295096.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-17	Caliber Collision Centers	TX	2/5/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 26, 2018, we learned of a "phishing" event in which an unidentified third party obtained unauthorized access to employee information through a malicious e-mail sent to our employees. The data accessed may have included employment, pay and benefits information, such as an employee's name, address, date of birth, Social Security number, bank account numbers, benefit selections and similar information stored on our Human Resources system.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Caliber Collision Centers
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295090.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-16	Aflac	GA	2/6/2018	Electronic	Business	Yes - Unknown #	Unknown

Accordingly, we are writing to inform you that we discovered that unauthorized access has been obtained to an Aflac associate's email account. Personal information that may have possibly been accessed are your name and social security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Aflac
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294982%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294982%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-15	DSW, Inc.	OH	2/7/2018	Electronic	Business	Yes - Unknown #	Unknown

On or about January 29, 2018, a cybercriminal accessed our system and used such access to send a phishing e-mail to a number of our employees. As a result of this unauthorized access, however, the cybercriminal may have obtained access to personal information for the affected employees, including their names, social security numbers, dates of birth, home addresses, phone numbers, personal e-mail addresses, wage information, or bank account information.

Attribution 1 Publication: MD AG's office Author:
Article Title: DSW, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294971.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-14	TrueNet Communications, Inc.	FL	2/8/2018	Electronic	Business	Yes - Unknown #	Unknown

Specifically, we recently discovered that an unauthorized third party gained access to a TrueNet employee's email credentials and redirected certain emails that contained employee and contractor information, which allowed the authorized third party to access the emails. Through our investigation, we have determined that the third party accessed the name and Social Security number relating to certain TrueNet employees and contractors.

Attribution 1 Publication: MD AG's office Author:
Article Title: TrueNet Communications, Inc.
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295094.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-13	Fontainebleau Miami Beach	FL	2/8/2018	Electronic	Business	Yes - Published #	158

On January 3, 2018, Fontainebleau Miami Beach ("Fontainebleau") learned that certain guests' credit card information was acquired without authorization. (Exposure number per NC AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office / NC AG Author:
Article Title: Fontainebleau Miami Beach
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294969.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-12	Norwich Commercial Group, Inc. dba Norcom Mortgage	CT	2/14/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On December 12, 2017, Norcom discovered that between October 12, 2017 and December 12, 2017, several of its employees' e-mail accounts may have been accessed by an unauthorized third-party. After reviewing the email messages that were potentially accessed, Norcom has determined that such e-mails may have contained the first and last names, Social Security numbers, bank account numbers and/or driver's license numbers of these residents.

Attribution 1 Publication: MD AG's office Author:
Article Title: Norwich Commercial Group, Inc. dba Norcom Mortgage
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295101.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-11	Belmont Savings Bank	MA	2/20/2018	Electronic	Banking/Credit/Financial	Yes - Published #	2,434

On November 30, 2017 the cleaners at Belmont Savings Bank Operations Center inadvertently discarded an unencrypted computer that contained account numbers, Social Security Numbers or Tax ID numbers (the "Personal Information"). (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office Author:
Article Title: Belmont Savings Bank
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295118.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-10	iMiller Public Relations LLC	NY	2/20/2018	Electronic	Business	Yes - Unknown #	Unknown

On November 6, 2017, iMiller learned that one of its employees may have been the victim of an email phishing attack. The information that was available in the potentially compromised email account included the Maryland resident's name and Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: iMiller Public Relations LLC
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295111.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-09	Rockville Eye Surgery Center, LLC dba Palisades Surgery Center	MD	2/20/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Please be advised, on January 23, 2018, our client, Rockville Eye Surgery Center, LLC d/b/a Palisades Surgery Center ("Palisades") learned that personal information may be subject to unauthorized access or acquisition as the result of a cyber-attack. The data elements involved may have included name, address, Social Security number, and medical information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Rockville Eye Surgery Center, LLC dba Palisades Surgery Center
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295057.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-08	JJ Haines	MD	2/21/2018	Electronic	Business	Yes - Unknown #	Unknown

The information contained on your 2017 W-2 may have been acquired by an unauthorized person. This includes you full name, address, Social Security Number and 2017 wage information.

Attribution 1 Publication: MD AG's office Author:
Article Title: JJ Haines
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295056.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-06	Meridian Group	MD	2/22/2018	Electronic	Business	Yes - Unknown #	Unknown

Meridian subsequently determined, with the help of outside computer forensic investigators, that an unknown actor had gained access to the Meridian employee's email account periodically between September 12, 2017 and October 12, 2017, likely as the result of a sophisticated phishing email. The email account may have contained the name, date of birth, address, Social Security Number, and financial account information of the affected Maryland residents.

Attribution 1 Publication: MD AG's office Author:
Article Title: Meridian Group
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295063.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-05	Musicians on Call, Inc.	TN	2/22/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 28, 2018, Musicians On Call learned that an employee's company laptop had been stolen during a home burglary. The laptop contents included data from records of past and present volunteers. We believe the information may have included: your name, phone number or address, either a driver's license or passport number, or a social security number.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
 Article Title: Musicians on Call, Inc.
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295062.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-04	Summit Inspection Services	CA	2/23/2018	Electronic	Business	Yes - Unknown #	Unknown

I am writing to inform you of a data security incident affecting the computer of a Summit Inspection Services employee. It appears that on or around December 2, 2017, an unauthorized person or persons gained access to the computer and attempted unsuccessfully to redirect several transactions. While the investigation continues, our current understanding is that the affected personal information may include your Social Security number, government-issued identification information (such as a driver's license number or Employer Identification Number), and bank account number.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Summit Inspection Services
 Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295072%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295072%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-03	Cedarville University	OH	2/26/2018	Electronic	Educational	Yes - Published #	241

During the investigation of what occurred, which included the direct involvement of the external software vendor and concluded February 14, Cedarville learned that a software error had occurred that resulted in a limited number of 2017 tax forms being potentially viewable by other Cedarville employees.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Cedarville University
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295108.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-02	ALCOVA Mortgage, LLC	WY	2/26/2018	Electronic	Banking/Credit/Financial	Yes - Published #	112

ALCOVA Mortgage, LLC ("ALCOVA") has discovered that three ALCOVA email addresses were exploited in a cyberattack. The information available differed based on the documentation needs of your specific application. In addition to your name, it could have included Social Security numbers, potentially including those of your dependents; banking account data; debit or credit card information; and your driver's license or other identification document. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office Author:
 Article Title: ALCOVA Mortgage, LLC
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295075.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180427-01	MorshedEye, PLLC	KY	4/13/2018	Electronic	Medical/Healthcare	Yes - Published #	1,100

MorshedEye, PLLC KY Healthcare Provider 1100 04/13/2018 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: MorshedEye, 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
ITRC20180426-13	Caroline County Office of the County Administrator - Office of Finance	MD	2/28/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

On February 5th an employee working in the Office of Finance received an email that appeared to come from the County Administrator. The email asked for a digital copy of the County's 2017 W-2 forms. A W-2 contains identifying information including the employee's name, address, wages, taxes paid, and social security number.

Attribution 1 Publication: MD AG's office Author:
 Article Title: Caroline County Office of the County Administrator - Office of Finance
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295084.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180426-12	LI Tax and Planning, Inc.	NY	4/19/2018	Electronic	Business	Yes - Published #	3,882

That forensic team determined that, on or about November 1, 2017, an unauthorized individual gained access to LIT78's computer system and exfiltrated a data file containing clients' personally identifiable information to a unfamiliar cloud service, Mega.nz. The file taken included certain LIT78 clients' full names, addresses, and social security numbers (SSN) along with their wage and other tax-related information. It also included many clients' telephone numbers, email addresses, and occupations. (Exposure number per MA OCABR)

Attribution 1 Publication: NH AG's office Author:
 Article Title: LI Tax and Planning, Inc.
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/li-tax-20180419.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180426-11	Firstmark Services	NE	4/9/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Our records indicate that on April 04, 2018, an email intended for another existing customer inadvertently included your information. The email sent included your first name and the above account number.

Attribution 1 Publication: NH AG's office Author:
 Article Title: Firstmark Services
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/firstmark-20180409.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180426-10	Riverside Medical Center	IL	4/20/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Riverside Medical Center IL Healthcare Provider Unknown 04/20/2018 Theft Desktop Computer, Other

Attribution 1 Publication: hhs.gov Author:
 Article Title: Riverside 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
ITRC20180426-08	Trust Company of the South	NC	4/24/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 19, 2018, we discovered that an unauthorized individual had gained access to our email system. Type of information exposed was not disclosed.

Attribution 1 Publication: VT AG's office Author:
 Article Title: Trust Company of the South
 Article URL: <http://ago.vermont.gov/blog/2018/04/24/trust-company-of-the-south-notice-of-data-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180426-07	Capital Digestive Care	MD	4/23/2018	Electronic	Medical/Healthcare	Yes - Published #	13,572

On February 23, 2018, we were notified that a third-party vendor stored data files on a commercial cloud server without adequate security, which were discovered by an individual who informed us of the incident. As a result of this investigation, it was determined that the information was limited to the "Schedule a Visit" and "Contact" pages on our website containing personal information you may have submitted, including your name, address, telephone number, email address, date of birth, and possible health information. (Exposure number per MA OCABR)

Attribution 1 Publication: NH AG's office Author:
 Article Title: Capital Digestive Care
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/capital-digestive-care-20180423.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180426-06	AccessLex Institute dba Access Group (Nelnet)	PA	4/18/2018	Electronic	Banking/Credit/Financial	Yes - Published #	16,500

On March 28, 2018 we learned that on March 23, 2018 a vendor we use to help provide student loan processing services inadvertently sent a copy of certain loan files, including your file, to another business that was not authorized to receive them. The information involved included your name, driver's license number, and Social Security number.

Attribution 1 Publication: CA AG's office / cbsnews.com Author:
 Article Title: AccessLex Institute dba Access Group
 Article URL: https://oag.ca.gov/system/files/CA%20notification%20letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180426-05	MEDantex	KS	4/23/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

MEDantex, a Kansas-based company that provides medical transcription services for hospitals, clinics and private physicians, took down its customer Web portal last week after being notified by KrebsOnSecurity that it was leaking sensitive patient medical records — apparently for thousands of physicians.

Attribution 1 Publication: krebsonsecurity.com Author:
 Article Title: ranscription Service Leaked Medical Records
 Article URL: <https://krebsonsecurity.com/2018/04/transcription-service-leaked-medical-records/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180426-04	Texas Health and Human Services	TX	4/25/2018	Electronic	Government/Military	Yes - Published #	100

The Texas Health and Human Services Commission's Office of the Inspector General is investigating how a former agency employee was mailed a box full of private client information. Tracy Ryans got mail — straight from the Texas Health and Human Services Commission, including a box full of state assistance application forms with hundreds of people's social security card numbers, green card certificates, billing statements, check stubs and photocopies of driver's licenses.

Attribution 1 Publication: texastribune.org Author:
 Article Title: Texas Health and Human Services
 Article URL: <https://www.texastribune.org/2018/04/25/texas-health-commission-employee-was-fired-then-she-received-private-i/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180426-03	Texas Health Physicians Group	TX	4/13/2018	Electronic	Medical/Healthcare	Yes - Published #	3,808

On January 17, 2018, law enforcement advised us that an unauthorized third party may have gained access to some Texas Health email accounts in October 2017. The investigation determined that some patients' information may have been in the affected email accounts, and may have included patients' names, medical record numbers, dates of birth, addresses, insurance information, clinical information, and in some instances Social Security numbers and driver's license and state identification numbers.

Attribution 1 Publication: THPG notification / hhs.gov Author:
 Article Title: Medical records of Texas Health patients may have been exposed in data breach
 Article URL: <https://www.thpg.org/Pages/A-Notice-to-Our-Patients.aspx>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180426-02	Cornerstone Foot & Ankle	NJ	4/16/2018	Electronic	Medical/Healthcare	Yes - Published #	533

Cornerstone Foot & Ankle NJ Healthcare Provider 533 04/16/2018 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: Cornerstone Foot & Ankle
 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
ITRC20180426-01	Center for Orthopaedic Specialists - Providence Medical Institute	CA	4/19/2018	Electronic	Medical/Healthcare	Yes - Published #	81,550

An unauthorized party gained access to the computer system used to house patient information, and then encrypted that information in an attempt to extort a monetary payment from COS. To the best of our knowledge, none of your personal information was removed or downloaded while COS's computer system was being accessed by the unauthorized party. In the unlikely event that your information was removed, that information could have included: Demographic or other information such as name, mailing address, date of birth, account number, etc., medical records and insurance information and Social Security numbers

Attribution 1 Publication: myidcare.com Notification / hhs.gov Author:
 Article Title: Center for Orthopaedic Specialists - Providence Medical Institute
 Article URL: <https://ide.myidcare.com/cos/frequently-asked-questions>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180423-09	American Esoteric Laboratories	AL	4/20/2018	Electronic	Medical/Healthcare	Yes - Published #	500

On October 15, 2017, a laptop issued to one of AEL's employees was stolen. Our investigation indicates that some of your personal information, which may include your name, address, Social Security number, date of birth, health insurance information, or medical treatment information, may have been stored on the laptop.

Attribution 1 Publication: VT AG's office / hhs.gov / NH AG's office Author:
 Article Title: Data breach could impact some patients of medical lab chain with Alabama locations
 Article URL: <http://ago.vermont.gov/blog/category/security-breaches/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180423-07	SunTrust Bank (2/12/18)	GA	2/12/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Prior to the former employee returning the laptop, our office was informed on October 26, 2017 that certain personal and account information (described below) had been accessed by the former employee through the laptop without authorization. Based on our findings, we confirmed that sensitive information (one Maryland resident's name, address, account number, date of birth, and Social Security number) was accessed after separation from the bank.

Attribution 1 Publication: MD AG's office Author:
 Article Title: SunTrust Bank
 Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295040.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180423-06	North Park University	IL	4/10/2018	Electronic	Educational	Yes - Unknown #	Unknown

The investigation determined that an unknown individual had access to a North Park University employee's email account between January 24, 2018 and February 22, 2018. The personal information contained in the employee's email account includes your name and Social Security number.

Attribution 1 Publication: NH AG's office Author:
 Article Title: North Park University
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/north-park-20180410.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180423-05	Institute for Supply Management	AZ	4/3/2018	Electronic	Business	Yes - Published #	246

Based on ISM's investigation to date, at this time we believe that, on or about January 25, 2018, an unauthorized sender caused "phishing" emails to be sent to email addresses contained in an ISM employee's email contacts list, which was contained on or accessed by a mobile computing device used by that employee for exchanging emails with certain ISM customers. (Exposure number per MA OCABR)

Attribution 1 Publication: NH AG's office Author:
Article Title: Institute for Supply Management
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/institute-for-supply-20180403.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180423-03	Eastern Bank (3/8)	MA	3/8/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 1, 2018, an A TM skimming device was discovered on an Eastern Bank ATM. Since that date, we have since discovered that three more ATM's were similarly compromised, impacting an additional five Eastern Bank New Hampshire customers (for a total impact often New Hampshire residents).

Attribution 1 Publication: NH AG's office Author:
Article Title: Eastern Bank (3/8)
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/eastern-bank-20180308.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180423-02	Illinois Department of Healthcare and Family Services and Illinois	IL	4/21/2018	Paper Data	Government/Military	Yes - Published #	8,000

The personal information of more than 4,000 people who were clients of two Illinois state agencies was inadvertently mailed to the wrong addresses. The leaked information, which included health insurance information, medical and financial information, and dates of birth, was addressed to the correct individual, but sent to the wrong addresses. (Number of records exposed per hhs.gov)

Attribution 1 Publication: abc7chicago.com / hhs.gov Author:
Article Title: Illinois agencies mailed personal health information of 4,000 people to wrong addresses
Article URL: <http://abc7chicago.com/health/illinois-agencies-mailed-personal-information-of-4000-people-to-wrong-addresses/3374>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180423-01	Irvington School District	NJ	4/18/2018	Electronic	Educational	Yes - Published #	1,200

Partial social security numbers of more than 1,200 employees at Irvington schools were distributed via email on Monday to an unknown number of recipients, according to the school district. The email included the names of current and former employees and their social security numbers with a few numbers replaced by dashes or asterisks, a copy of the email obtained by NJ Advance Media shows.

Attribution 1 Publication: nj.com Author:
Article Title: Hacker sent email with 1,200 partial social security numbers to school staff
Article URL: http://www.nj.com/essex/index.ssf/2018/04/partial_social_security_numbers_for_1200_school_em.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180422-02	Lydia Security Monitoring dba COPS Monitoring	NJ	2/28/2018	Electronic	Business	Yes - Published #	2,260

On February 15, 2018, Lydia Security discovered that it was the victim of an email spoofing attack by an individual pretending to be a Lydia Security Executive. Unfortunately, copies of all 2016 and 2017 employee W-2 forms were provided before Lydia Security discovered that the request was made from a fraudulent account. (Exposure number per NC AG's office)

Attribution 1 Publication: MD AG's office Author:
Article Title: Lydia Security Monitoring dba COPS Monitoring
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295055.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180422-01	Teachers Insurance and Annuity Association (TIAA)	NY	4/17/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Recently, TIAA became aware that your personal identifiable information was viewed online by an unauthorized third-party. Your name, account balance, and Social Security number was viewed.

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: Teachers Insurance and Annuity Association (TIAA)
Article URL: <https://dojmt.gov/wp-content/uploads/TIAA-1.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180420-06	Frost Bank (multiple commercial customers)	TX	3/16/2018	Electronic	Banking/Credit/Financial	Yes - Published #	470

In March 2018, Frost detected unauthorized access into a third-party lockbox software program that allowed unauthorized users to view and copy images of checks stored electronically in the image archive. Our investigation determined that check images were the focus of the unauthorized access. The personal information that was accessed without authorization may include your name, address, bank account number, routing number, and any other information visible on the face of your check, as well as any information you may have included in the mailing with your check.

Attribution 1 Publication: Frost Bank website Author:
Article Title: Frost Bank (multiple commercial customers)
Article URL: <https://www.frostbank.com/newsroom/03-16-2018>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180420-05	SunTrust Bank (4/20/18)	GA	4/20/2018	Electronic	Banking/Credit/Financial	Yes - Published #	1,500,000

SunTrust announced Friday that a former employee may have tried to steal and share data of about 1.5 million customers, including names, addresses, phone numbers and account balances.

Attribution 1 Publication: fortune.com / IA AG's office / NH AG's of Author:
Article Title: Ex-SunTrust Employee May Have Tried Sharing 1.5 Million Customers' Data
Article URL: <http://fortune.com/2018/04/20/suntrust-bank-security-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180420-03	Control Technologies, Inc.	AL	4/9/2018	Electronic	Business	Yes - Unknown #	Unknown

On or about April 4, 2018, CTI became aware that it had been affected by a breach on February 22, 2018. It realized that it had been subject to an email attack when forged emails were being sent to a CTI employee's email accounts from someone appearing to be a company executive. mmediately contacted its IT Manager who blocked the emails, and it has contacted the authorities. Through the programmatic and manual review of an employee email account, the company determined that the information related to some employees and included their names, addresses, Social Security numbers and earnings information that was contained in the email account at the time it was accessed by the unknown individual(s).

Attribution 1 Publication: NH AG's office Author:
Article Title: Control Technologies, Inc.
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/control-technologies-20180409.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180420-02	Strategic Analysis, Inc.	VA	4/19/2018	Electronic	Business	Yes - Published #	2,074

During the course of the investigation, we became aware of unauthorized access to a number of SA accounts, systems, and data beginning April 20, 2015 and continuing through January 16, 2018. We identified that the data that could have been subject to unauthorized access includes your bank account number and routing number. (Exposure number per MA OCABR)

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Strategic Analysis, Inc.
Article URL: <http://ago.vermont.gov/blog/2018/04/19/strategic-analysis-inc-notice-of-data-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180420-01	Michael Gruber DMD PA	NJ	4/19/2018	Electronic	Medical/Healthcare	Yes - Published #	4,624

On February 20, 2018, Michael Gruber DMD PA discovered an unknown individual(s) gained access to Michael Gruber DMD PA's information system. Some of the emails accessible to the authorized individual(s) contained your name and other personal information.

Attribution 1 Publication: VT AG's office / hhs.gov Author:
Article Title: Michael Gruber DMD PA
Article URL: <http://ago.vermont.gov/blog/2018/04/19/michael-gruber-dmd-pa-notice-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180419-08	Victoria Independent School District	TX	4/10/2018	Electronic	Educational	Yes - Published #	35,108

Victoria ISD has learned that between July and October of 2017, emails within email accounts belonging to some of its employees may have been accessed without authorization. Our investigation indicates that some of your personal information, which may include your name, address, Social Security number, government-issued identification number, financial account information, and/or medical information, may have been contained in the affected email accounts. (Exposure number per MA OCABR)

Attribution 1 Publication: NH AG's office Author:
Article Title: Victoria Independent School District
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/victoria-independent-school-20180410.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180419-07	Polk County Health Services, Inc. / Crisis Observation Center	IA	4/16/2018	Electronic	Government/Military	Yes - Published #	1,071

During this period, Polk County Health Services, Inc. accidentally and unknowingly disseminated personal and protected health information of individuals who have received services at the Crisis Observation Center in Des Moines, Iowa. Polk County Health Services, The information unknowingly disclosed includes: full name, home address, Social Security number, Medicaid identification number, date of admission to the Crisis Observation Center and discharge location.

Attribution 1 Publication: PCHS press release / IA AG's office Author:
Article Title: Polk County Health Services, Inc. / Crisis Observation Center
Article URL: <https://businessrecord.com/Content/Default/All-Latest-News/Article/Data-breach-affects-hundreds-of-Polk-County-Cris>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180419-06	MedWatch, LLC	FL	4/13/2018	Paper Data	Medical/Healthcare	Yes - Published #	506

MedWatch recently learned that one of its vendors unintentionally misconfigured MedWatch's online portal which resulted in certain information being potentially accessible via internet search engines during the time period from October 20, 2017 until December 15, 2017. The information that was accessible may have included: members' full name, Social Security number, date(s) of service, employer group health plan name, date of birth, and providers' full names. (Exposure number per MA OCABR)

Attribution 1 Publication: Website Notice / hhs.gov Author:
Article Title: MedWatch, LLC
Article URL: <https://ide.myidcare.com/medwatch/frequently-asked-questions>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180419-05	B.T.C.E. dba HomeBrewIt.com	IN	4/16/2018	Electronic	Business	Yes - Published #	1,024

I am writing to inform you of a recent security incident involving the hosting company of our website. Our hosting company identified that an unauthorized party was able to gain access to their environment and execute malicious code on our website, HomeBrewIt.com. The execution of this malicious code led to sensitive customer information being exposed. The compromised data may have included your name, address and payment card information. (Exposure number per MA OCABR)

Attribution 1 Publication: VT AG's office Author:
Article Title: B.T.C.E. dba HomeBrewIt.com
Article URL: <http://ago.vermont.gov/blog/2018/04/16/btce-inc-sbn-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180419-04	Temp-Tations Home LLC dba Tara at Home	PA	4/16/2018	Electronic	Business	Yes - Published #	7,028

On December 12, 2017, we were notified by the vendor that hosts our e-commerce system, including the www.tarahome.com website, that an unknown third party had compromised individual online user accounts. The investigation determined that the unknown third party accessed certain online user accounts and may have accessed your name, payment card number, and the expiration date from payment cards used on the Tara at Home website from August 1, 2017 to December 1, 2017. (Exposure number per MA OCABR)

Attribution 1

Publication: VT AG's office

Author:

Article Title: Temp-Tations Home LLC dba Tara at Hom

Article URL: <http://ago.vermont.gov/blog/2018/04/16/temp-tations-home-llc-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180419-03	Carolina Digestive Health Associates	NC	4/18/2018	Electronic	Medical/Healthcare	Yes - Published #	10,988

On January 10, 2018, CDHA was contacted by the Charlotte-Mecklenburg Police Department and was told by the police they had discovered that a CDHA employee had stolen personal information belonging to some patients. (Number of records exposed per hhs.gov)

Attribution 1

Publication: CDHA website / VT AG's office / hhs.gov Author:

Article Title: Healthcare employee gave patient information to fraud suspects, police say

Article URL: <https://carolinadigestive.com/uploads/files/CDH-Substitute-Notice-Short-Form.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180419-02	Localblox	WA	4/18/2018	Electronic	Business	Yes - Unknown #	Unknown

The collected data was stored in an unsecured and unlisted Amazon S3 container, which was discovered by ethical data breach hunter Chris Vickery at cybersecurity research firm UpGuard. "The data collected includes names and physical addresses, and employment information and job histories data scraped from Facebook and LinkedIn profiles — like dates of birth and other public profile data, and Twitter handles," ZDNet reported after examining the files Vickery collected. The combined files amounted to 1.2 terabytes of storage, and up to 48 million user profiles were kept without a password.

Attribution 1

Publication: digitaltrends.com

Author:

Article Title: Localblox data breach is the latest nightmare for Facebook, LinkedIn

Article URL: <https://www.digitaltrends.com/computing/localblox-data-breach-hits-facebook-linkedin-twitter/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180419-01	TaskRabbit, Inc. (Ikea)	CA	4/14/2018	Electronic	Business	Yes - Unknown #	Unknown

On April 12, 2018, TaskRabbit learned that an unauthorized party gained access to its systems. Based on the investigation to date, TaskRabbit believes there may have been access to the following kinds of information for different users: name, website username and password, date of birth, truncated payment card, social security number, and/or bank account number.

Attribution 1

Publication: CA AG's office/NH AG's office/IA AG's o Author:

Article Title: TaskRabbit, Inc. (Ikea)

Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/taskrabbit-20180514.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180416-03	Bio-Rad Laboratories, Inc. (Dun & Bradstreet)	CA	4/4/2018	Electronic	Medical/Healthcare	Yes - Published #	362

On March 2, 2018, a service provider of ours, Dunn & Bradstreet, notified us that it had recently learned that it had been the target of an unauthorized third party intrusion. Specifically, the service provider explained that an unauthorized third party had used compromised credentials to log into the email accounts of a limited number of its employees in June 2017, and may have had access to personal information about our partners. We understand that the following elements of information may have been compromised: your name, address, telephone number, and Social Security number or individual tax identification number. (Exposure number per MA OCABR)

Attribution 1

Publication: NH AG's office

Author:

Article Title: Bio-Rad Laboratories, Inc. (Dun & Bradstreet)

Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/bio-rad-20180404.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180416-02	Iditarod Trail Committee	AK	4/14/2018	Electronic	Business	Yes - Unknown #	Unknown

Officials with the Iditarod Trail Committee say more than 100 race volunteers may have had their personal information compromised after a computer theft on March 11. According to a letter sent to each volunteer, the data that may have been accessed included full names and social security numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Iditarod Trail Committee
Article URL:

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180416-01	UnityPoint Health	IA	4/16/2018	Electronic	Medical/Healthcare	Yes - Published #	16,429

Access to the employee email accounts was first gained on November 1, 2017 and continued for a period of three months until February 7, 2018, when the phishing attack was detected and access to the compromised email accounts was blocked. The investigation revealed a wide range of protected health information had potentially been obtained by the attackers, which included names in combination with one or more of the following data elements: Medical record number, date of birth, service dates, treatment information, surgical information, lab test results, diagnoses, provider information, and insurance information.

Attribution 1 Publication: hipaajournal.com / WI AG's office Author:
Article Title: Several Employee Email Accounts Compromised in UnityPoint Health Phishing Attack
Article URL: <https://www.hipaajournal.com/several-employee-email-accounts-compromised-in-unitypoint-health-phishing-attack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-14	John Y. Trent & Associates, LLC	NY	4/4/2018	Electronic	Business	Yes - Published #	3,348

On March 1, 2018, JYT' s investigation determined that on September 29, 2017, an unauthorized actor or actors accessed a JYT workstation storing 2016 tax returns with client personal information and removed copies of this information. The data subject to unauthorized access varied by individual but can include the following: name, address, Social Security number, wage/salary information, date of birth, driver's license number and bank account information. (Exposure number per MA OCABR)

Attribution 1 Publication: NH AG's office Author:
Article Title: John Y. Trent & Associates, LLC
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/john-y-trent-20180404.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-13	Target Direct Marketing	MO	4/11/2018	Electronic	Business	Yes - Unknown #	Unknown

In an incident that calls to mind multiple data breaches in the analytics and influencing industries, the UpGuard Cyber Risk Team can now report that data relating to a number of subsidiaries of Kansas City holding company Blue Chair LLC, such as lead generation company Target Direct Marketing, was left exposed online, revealing personally identifiable information for over one million individuals seeking further information about higher education. The table "peg_historical" lists these consumers, alongside their names, home addresses, home and mobile phone numbers, email addresses, and, tellingly, some information about their educational backgrounds.

Attribution 1 Publication: upguard.com Author:
Article Title: Target Direct Marketing
Article URL: <https://www.upguard.com/breaches/rsync-tdm>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-12	Suncoast Hospital (now owned by Largo Medical Center)	FL	4/13/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

In room after room, we found old medicine vials, needles, collapsed ceilings and old medical records. The corporation that owned the closed facility has been inactive since 2012, but it is still responsible for the records.

Attribution 1 Publication: wfla.com Author:
Article Title: Former Suncoast Hospital patients worried about abandoned medical records
Article URL: <http://www.wfla.com/news/pinellas-county/former-suncoast-hospital-patients-worried-about-abandoned-medical-recor>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-11	CollegePlannerPro	CA	4/13/2018	Electronic	Business	Yes - Unknown #	Unknown

User names, email addresses, phone numbers, and other information belonging to independent college consultants who used CollegePlannerPro from 2015 to 2017 were freely available to anyone on web servers used by the software company.

Attribution 1 Publication: chronicle.com Author:
 Article Title: College Consultants' Client Information Was Exposed on Web Servers
 Article URL: <https://www.chronicle.com/article/College-Consultants-Client/243127>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-10	Texas Health Resources	TX	4/14/2018	Electronic	Medical/Healthcare	Yes - Published #	4,000

On January 17, 2018, law enforcement advised us that an unauthorized third party may have gained access to some Texas Health email accounts in October 2017. The investigation determined that some patients' information may have been in the affected email accounts, and may have included patients' names, medical record numbers, dates of birth, addresses, insurance information, clinical information, and in some instances Social Security numbers and driver's license and state identification numbers.

Attribution 1 Publication: Company website / hipaajournal.com Author:
 Article Title: A Notice to Our Patients Regarding an Email Account Incident
 Article URL: <https://www.thpg.org/Pages/A-Notice-to-Our-Patients.aspx>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-09	Prestera Center for Mental Health Services, Inc.	WV	3/20/2018	Electronic	Medical/Healthcare	Yes - Published #	670

Prestera Center for Mental Health Services, Inc. WV Healthcare Provider 670 03/20/2018 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
 Article Title: Prestera Center for Mental Health Services, 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
ITRC20180415-08	Children's National Medical Center	DC	3/30/2018	Electronic	Medical/Healthcare	Yes - Published #	722

Children's National Medical Center DC Healthcare Provider 722 03/30/2018 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
 Article Title: Children's National 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
ITRC20180415-07	Guardian Pharmacy of Jacksonville, LLC	GA	3/30/2018	Electronic	Medical/Healthcare	Yes - Published #	11,521

Guardian Pharmacy of Jacksonville, LLC ("Guardian") is notifying certain patients of the unauthorized access to certain limited pieces of patient information, including patient name, prescription medication information, treatment details, and diagnosis information. As part of Guardian's immediate and ongoing investigation into the event, on February 14, 2018, it was determined that certain pieces of patient information were accessible to an unauthorized individual(s).

Attribution 1 Publication: Guardian website / hhs.gov Author:
 Article Title: Guardian Jacksonville Notifies Patients of Email Compromise
 Article URL: <http://www.guardianpharmacyflorida.com/general-news/guardian-jacksonville-notifies-patients-of-email-compromise/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-06	Quality Care Pharmacy	CA	4/2/2018	Paper Data	Medical/Healthcare	Yes - Published #	2,000

Professional thieves targeted the pharmacy, located in a San Marcos strip mall, and stole hundreds of thousands of dollars of medications and a computer containing unencrypted protected health information.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: Quality Care Pharmacy
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
ITRC20180415-05	Diagnostic Radiology & Imaging, LLC	NC	4/5/2018	Electronic	Medical/Healthcare	Yes - Published #	800

An investigation revealed that on November 11, 2017, an employee of DRI became the victim of a phishing attack. Within that DRI employee's email account, we found a limited amount of information about patients, including names, a general description of imaging services received (including date, type, and location of imaging service), medical record numbers, and in some cases, email addresses and phone numbers. In just a few cases, the patient's date of birth was also included.

Attribution 1 Publication: DRI website notice / hhs.gov Author:
Article Title: Diagnostic Radiology & Imaging, LLC
Article URL: <https://www.greensboroimaging.com/2018/03/30/important-notice-phishing-attack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-04	Mise En Place Restaurant Services, Inc.	CA	4/12/2018	Electronic	Business	Yes - Published #	27,997

On March 15, 2018, MEP discovered that part of its network was potentially subject to a ransomware attack. The information may have included: full name; address; Social Security or Federal Identification Number; passport, driver's license, or resident card number; bank account and routing number; and the login information for a bank account, insurance or vendors, if provided to MEP. (Exposure number per MA OCABR)

Attribution 1 Publication: CA AG's office / Company Press Release Author:
Article Title: Mise En Place Restaurant Services, Inc.
Article URL: <https://www.prnewswire.com/news-releases/mise-en-place-restaurant-services-inc-notifies-clients-individuals-followin>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-03	Pierre Fabre (PF@-com, Inc.)	NJ	4/13/2018	Electronic	Business	Yes - Published #	4,423

On March 12, 2018, we discovered that information entered on some of our websites (aveneusa.com, renefurtererusa.com, kloraneusa.com, and glytone-usa.com (the "Websites")) had been captured and potentially sent to unauthorized third parties. Based on our investigation, the following types of personal information may have been exposed during this time: name, credit or debit card information or other payment account information, phone number, email address, shipping address, billing address and/or Website account password. (Exposure number per MA OCABR)

Attribution 1 Publication: CA AG's office Author:
Article Title: Pierre Fabre (PF@-com, Inc.)
Article URL: https://oag.ca.gov/system/files/CA%20-%20Notification%20of%20Breach_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-02	Inogen	CA	4/13/2018	Electronic	Medical/Healthcare	Yes - Published #	29,528

On March 14, 2018, Inogen learned that messages within an employee email account may have been accessed without authorization and that some of those messages may have contained personal information belonging to some Inogen rental customers. It appears that customer names, addresses, telephone numbers, email addresses, dates of birth, dates of death, Medicare identification numbers, insurance policy information, and/or the type of medical equipment provided may have been accessed. (Exposure number per IN AG's office)

Attribution 1 Publication: CA AG's office / beckershospitalreview.c Author:
Article Title: Inogen
Article URL: https://oag.ca.gov/system/files/Inogen%20-%20CA%20Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180415-01	Blue Shield of California	CA	4/13/2018	Electronic	Medical/Healthcare	Yes - Published #	1,717

On March 23, 2018, the Blue Shield of California (Blue Shield) Privacy Office received confirmation that your Protected Health Information had been shared with an insurance broker who was not authorized to receive it. The Protected Health Information (PHI) disclosed included only the following: your name, home address, mailing address, Blue Shield subscriber identification number, telephone number, and the name of the Blue Shield Medicare Advantage plan you were enrolled in at the time.

Attribution 1 Publication: CA AG's office Author:
Article Title: California Physician's Service dba Blue Shield of California
Article URL: https://oag.ca.gov/system/files/Notice%20Letter%20Template%20Final_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180412-04	Integrated Rehab Consultants	IL	4/12/2018	Electronic	Medical/Healthcare	Yes - Published #	4,292

On December 2, 2016, Integrated Rehab Consultants ("IRC") was contacted by a healthcare researcher regarding IRC data that was present on a public repository. The information that was visible on the public repository includes IRC patients' full name, visit date, medical provider information, date of birth, gender, visit status, address, admission date, treatment location, appointment visit ID, diagnosis codes, and procedure code.

Attribution 1 Publication: IRC press release Author:
Article Title: Integrated Rehab Consultants Takes 16 Months to Notify Patients of PHI Breach
Article URL: <https://www.prnewswire.com/news-releases/integrated-rehab-consultants-notice-of-data-security-incident-300626764>.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180412-03	NYC Health + Hospitals/Harlem	NY	3/29/2018	Electronic	Medical/Healthcare	Yes - Published #	595

The possible disclosure-a laptop computer missing from the facility-occurred on January 25, 2018, and was discovered on January 29. The PHI on the laptop included patients' names, medical record numbers, dates of birth, and whether a hearing test was passed.

Attribution 1 Publication: hhs.gov / NYC Health + Hospitals websit Author:
Article Title: NYC Health + Hospitals/Harlem
Article URL: <https://www.nyhealthandhospitals.org/pressrelease/notification-of-possible-phi-disclosure-2/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180412-02	Sonoma County Indian Health Project, Inc.	CA	3/30/2018	Electronic	Medical/Healthcare	Yes - Published #	662

Sonoma County Indian Health Project, Inc CA Healthcare Provider 662 03/30/2018 Unauthorized Access/Disclosure Desktop Computer, Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Sonoma County Indian Health Project, 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
ITRC20180412-01	West Kendall Baptist Hospital	FL	4/2/2018	Electronic	Medical/Healthcare	Yes - Published #	1,480

A former employee of Baptist Health's West Kendall Baptist Hospital in Miami, FL has been discovered to have stolen the credit card details of at least one patient and used the information to make fraudulent purchases. Any patient who paid for medical services using a credit card with the registration employee between August 2014 and March 2018 have potentially had their name, date of birth, and credit card details stolen and misused.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Baptist Health Alerts Almost 1,500 Patients to Possible Abuse of Credit Card Details
Article URL: <https://www.hipaajournal.com/baptist-health-alerts-almost-1500-patients-to-possible-abuse-of-credit-card-details/>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180411-04	Springer Science and Business Media LLC	NY	4/3/2018	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that one of our employees inadvertently sent to an unintended recipient an email containing certain individuals' tax information, including yours.

Attribution 1 Publication: VT AG's office Author:

Article Title: Springer Science and Business Media LLC

Article URL: <http://ago.vermont.gov/blog/2018/04/03/springer-science-and-business-media-llc-security-notification-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180411-03	Lincoln Financial Group	PA	4/3/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Lincoln recently discovered that one of its employees was the victim of a phishing attack which resulted in a third party gaining limited unauthorized access to the employee's account for a period of time between Feb. 8 and 9, 2018. Based on the facts known to Lincoln at this time, the personal information affected by this unauthorized access may have included a combination of your name, address, date of birth, driver's license number, policy number, Social Security number and/or health information.

Attribution 1 Publication: MT AG's office Author:

Article Title: Lincoln Financial Group (2/8/18)

Article URL: <https://dojmt.gov/wp-content/uploads/Lincoln-Financial-Group.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180411-02	Bearing Distributors, Inc.	OH	4/6/2018	Electronic	Business	Yes - Published #	857

On March 30, 2018, we discovered that our company was the victim of an email spoofing attack that same day by an individual pretending to be our President and CEO. A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information related to you as a BDI employee: (1) name; (2) address; (3) Social Security number; and (4) wage information. (Exposure number per MA OCABR)

Attribution 1 Publication: MT AG's office Author:

Article Title: Bearing Distributors, Inc.

Article URL: <https://dojmt.gov/wp-content/uploads/Bearing-Distributors-Inc.-BDI.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180411-01	LPL Financial (4/10/18)	MA	4/10/2018	Electronic	Banking/Credit/Financial	Yes - Published #	297

On February 28, 2018, we learned that an unauthorized individual obtained access to the system at LPL that your advisor uses to manage his clients' accounts. The system contained some of your personal information, including your name, address, date of birth, Social Security number, LPL account number and other account-related information, and if you maintain wire instructions on your LPL account, your banking account and routing numbers. (Exposure number per MA OCABR)

Attribution 1 Publication: MT AG's office Author:

Article Title: LPL Financial (4/10/18)

Article URL: <https://dojmt.gov/wp-content/uploads/LPL-Financial-LLC.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180410-03	Friedman, Leavitt & Associates, Inc. (CPA)	OH	3/27/2018	Electronic	Business	Yes - Unknown #	Unknown

On February 10 and 11, an unauthorized party accessed our computer system and was able to view and, potentially, download some client information over a period of approximately 12 hours. It is possible that the intruder viewed and downloaded certain of your personal identifiable information including possibly your name, address, social security number, and birthdate.

Attribution 1 Publication: VT AG's office / MD AG's office Author:

Article Title: Friedman, Leavitt & Associates, Inc. (CPA)

Article URL: <http://ago.vermont.gov/blog/2018/03/27/friedman-leavitt-associates-inc-sbn-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180410-02	Ithaca College (11/28/17)	NY	3/14/2018	Electronic	Educational	Yes - Published #	143

During the investigation, we determined certain Ithaca email accounts were logged into by unauthorized actors between July 14 and December 15, 2017, as the result of email phishing attacks that stole employee email account credentials. Type of information exposed was not disclosed. (Exposure number per NC AG's office)

Attribution 1 Publication: VT AG's office Author:
Article Title: Ithaca College (11/28/17)
Article URL: <http://ago.vermont.gov/blog/2018/03/14/ithaca-college-notice-of-data-security-breach-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180410-01	Archbright	WA	4/6/2018	Paper Data	Business	Yes - Unknown #	Unknown

On February 21, 2018, we discovered unauthorized acquisition by a third party to certain pension recipient paper records in the possession of a work-from-home employee. Type of information exposed was not disclosed.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180409-08	Cross Road Health Ministries, Inc.	AK	3/30/2018	Electronic	Business	Yes - Published #	245

On January 17, 2018, we discovered that a purported technical support company that on several occasions was allowed to connect remotely to our computer network for the purpose of resolving computer software issues, was part of a fraudulent scamming operation. We determined that during a purported support session, a file containing some of your personal information associated with payroll may have been accessible, which may have included your name, date of birth, Social Security number, and financial account information used for direct deposit. (Exposure number per IN AG's office)

Attribution 1 Publication: NH AG's office Author:
Article Title: Cross Road Health Ministries, Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/cross-road-health-20180330.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180409-07	Boys & Girls Club of Wake County	NC	3/26/2018	Electronic	Business	Yes - Unknown #	Unknown

In connection with a recent investigation, the Boys & Girls Clubs became aware that an unauthorized third party gained access to certain servers on our network and installed malware on certain servers. Based on this investigation, we believe this incident may have involved some or all of the following information: your first and last name; your Social Security number; your driver's license number; and certain financial account information.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Boys & Girls Club of Wake County
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/boys-and-girls-20180326.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180409-06	Bigfoot Gun Belts	ID	3/23/2018	Electronic	Business	Yes - Published #	4,141

As a result of this review, we learned that certain customer credit and debit card information may have been obtained by an unauthorized party from our payment portal when purchasing through our online store at www.gunbelts.com, from October 31, 2017 through February 1, 2018. Based on our investigation, the information potentially involved in this incident may have included your name, credit or debit card number, and card expiration date. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office Author:
Article Title: Bigfoot Gun Belts
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/bigfoot-gun-belts-20180323.pdf>



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

Report Date: 7/2/2018

Page 78 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180409-05	Fondren Orthopedic Group, LLP	TX	4/2/2018	Paper Data	Medical/Healthcare	Yes - Published #	11,552

Fondren Orthopedic Group L.L.P. TX Healthcare Provider 11552 04/02/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: Fondren Orthopedic Group, 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
ITRC20180409-03	Blue Beacon	CA	4/6/2018	Electronic	Business	Yes - Published #	33,644

On March 15, 2018, we discovered that our employee portal accounts had been accessed without authorization. Information involved included current and former employees' Social Security numbers and portal login credentials. (Exposure number per MA OCABR)

Attribution 1 Publication: CA AG's office / MT AG's office Author:
 Article Title: Blue Beacon
 Article URL: https://oag.ca.gov/system/files/Blue%20Beacon--CA%20Adult%20Consumer%20Notification%20Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180409-02	Chesapeake Regional Healthcare Sleep Center	VA	4/6/2018	Electronic	Medical/Healthcare	Yes - Published #	2,100

The letter is serving to inform patients about a data breach involving two unencrypted, portable hard drives containing each patient's name, date of birth and unique patient identification number produced by Chesapeake Regional Healthcare, plus demographic information, medications prescribed, and details of procedures that were performed at the CRH Sleep Center.

Attribution 1 Publication: Company website / hipaajournal.com / h Author:
 Article Title: Portable Hard Drives Missing from Chesapeake Regional Healthcare
 Article URL: <https://chesapeakeregional.com/patients-visitors/sleep-center-breach-information>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180409-01	California Department of Developmental Services	CA	4/6/2018	Paper Data	Government/Military	Yes - Published #	582,000

On Sunday, February 11, 2018, unknown persons broke into the Department's legal and audits offices, ransacked the offices and paper files, vandalized property, and started a fire. Some of the paper documents displaced or damaged in the fire included personal information of employees of regional centers and service providers, applicants seeking employment with the Department's audits office, and parents of minors enrolled in DDS fee programs.

Attribution 1 Publication: CA AG's office / hhs website Author:
 Article Title: California disability clients, state employees hit by data breach
 Article URL: https://oag.ca.gov/system/files/ddsBreachNoticePII_English_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180405-02	California Veterans Affairs Health Care System (VA Palo Alto Health Care System)	CA	3/26/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

The notification said that the Palo Alto Health Care System sent out letters to veterans that had one veteran's name but another's address on the envelopes. Type of information exposed was not disclosed.

Attribution 1 Publication: military.com Author:
 Article Title: VA Data Breach Reported by California Hospital
 Article URL: <https://www.military.com/militaryadvantage/2018/03/26/va-data-breach-reported-california-hospital.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180405-01	ai (multiple companies)	CA	4/5/2018	Electronic	Business	Yes - Unknown #	Unknown

ai discovered and contained an incident potentially affecting the online customer payment information of a small number of our client companies, and affected clients have been notified.

Attribution 1 Publication: [24]7.ai press release Author:
Article Title: [24]7.ai Issues Statement on Information Security
Article URL: <https://www.prnewswire.com/news-releases/247ai-issues-statement-on-information-security-300624659.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180404-09	Wisconsin Department of Health Services (The Management Group)	WI	4/4/2018	Electronic	Government/Military	Yes - Published #	779
<p>The Department of Health Services (DHS) and The Management Group (TMG) are notifying IRIS participants of a breach of information due to theft of a laptop and a work bag of a TMG IRIS Consultant on February 5. TMG found the laptop may have contained personal information about IRIS participants, including names, addresses, dates of births, participation in IRIS, services, Medicaid numbers, financial information, and social security numbers.</p>							

Attribution 1 Publication: DHS website / WI AG's office Author:
Article Title: Department of Health Services and The Management Group Announce Breach of Information
Article URL: <https://www.dhs.wisconsin.gov/news/releases/040418.htm>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180404-08	Mentor ABI, LLC	MA	3/21/2018	Electronic	Medical/Healthcare	Yes - Published #	994
<p>Mentor ABI, LLC MA Healthcare Provider 994 03/21/2018 Loss Other Portable Electronic Device</p>							

Attribution 1 Publication: hhs.gov Author:
Article Title: Mentor ABI, 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
ITRC20180404-07	Center for Comprehensive Services, Inc. dba NeuroRestorative Maryland	MA	3/21/2018	Electronic	Medical/Healthcare	Yes - Published #	1,176
<p>On or around December 23, 2017, these entities discovered that an unencrypted disk sent to them by their third-party software provider (Bullpen Financial, Inc.) containing documents that included sensitive information appeared to have been lost in the mail.</p>							

Attribution 1 Publication: MD AG's office / hhs.gov Author:
Article Title: Center for Comprehensive Services, Inc. dba NeuroRestorative Maryland (Bullpen Financial, Inc.)
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295289.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180404-06	North Beach School District	WA	2/1/2018	Electronic	Educational	Yes - Unknown #	Unknown

Last night we learned that there was a personal data breach in our district at approximately ten o'clock Tuesday, January 30. Someone posing as the superintendent requested via email a PDF listing of all employee names, addresses, salary information and social security numbers.

Attribution 1 Publication: WA AG's office Author:
Article Title: North Beach School District
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Home/Supporting_Law_Enforcement/NorthBeachSchoolDi

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180404-04	Panerabread.com	MO	4/2/2018	Electronic	Business	Yes - Unknown #	Unknown

Panerabread.com, the Web site for the American chain of bakery-cafe fast casual restaurants by the same name, leaked millions of customer records — including names, email and physical addresses, birthdays and the last four digits of the customer's credit card number — for at least eight months before it was yanked offline earlier today, KrebsOnSecurity has learned.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Panerabread.com Leaks Millions of Customer Records
Article URL: <https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180404-02	Autism Learning Partners Holdings, Inc. (A is for Apple)	CA	4/3/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On March 15, 2018, A is for Apple sent an email to a former employee in response to her request for a copy of her 2017 IRS Form W-2. Instead of sending only the former employee's W-2, the response inadvertently included an attachment with the W-2 forms for all current and former employees, including yours.

Attribution 1 Publication: CA AG's office / VT AG's office Author:
 Article Title: Autism Learning Partners Holdings, Inc. (A is for Apple)
 Article URL: https://oag.ca.gov/system/files/ALP-AisforApple_Sample_Notice_04-03-18_1.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180404-01	Milligan Chiropractic Group dba Del Mar Chiropractic Sports Group	CA	3/30/2018	Electronic	Medical/Healthcare	Yes - Published #	2,640

On January 31, 2018, we discovered that an employee's laptop computer was stolen. Although the laptop was password protected and we are not aware of the misuse of your or anyone's information, we could not rule out the possibility that your personal information, including your name, date of birth, clinic notes, and progress notes may be at risk.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
 Article Title: Milligan Chiropractic Group dba Del Mar Chiropractic Sports Group
 Article URL: https://oag.ca.gov/system/files/CA%20Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180403-01	Hudson Bay Company dba Saks Fifth Avenue Lord & Taylor and Saks OFF 5th	NY	4/1/2018	Electronic	Business	Yes - Published #	5,000,000

We recently became aware of a data security issue involving customer payment card data at certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores in North America.

Attribution 1 Publication: Saks Fifth Avenue statement / NH AG's Author:
 Article Title: Card Data Stolen From 5 Million Saks and Lord & Taylor Customers
 Article URL: <https://mobile.nytimes.com/2018/04/01/technology/saks-lord-taylor-credit-cards.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-24	Cohen, Bergman, Klepper & Romano	NY	3/26/2018	Electronic	Medical/Healthcare	Yes - Published #	42,000

The UpGuard Cyber Risk Team can now confirm that a digital data repository containing records from a Long Island medical practice was left publicly accessible, revealing medical details and personally identifiable information for over forty-two thousand patients. The presence of physicians' personal information in the files, such as their Social Security numbers and addresses, as well as over three million "medical notes," each one a physician's observation of a patient - such as a blood pressure measurement or a comment about a patient's reflexes - further widens the exposure's reach.

Attribution 1 Publication: Upguard.com Author:
 Article Title: Health Risk: How a Medical Practice Exposed Details for 40,000 Patients
 Article URL: <https://www.upguard.com/breaches/rsync-medical>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-23	Middletown Medical PC	NY	3/28/2018	Electronic	Medical/Healthcare	Yes - Published #	63,551

On January 29, 2018, we learned that the security setting on a Middletown Medical radiology interface may have permitted users to see a patient listing, which included your name, birthdate, client identification number, an indication that you received radiology services, and the date(s) when you received those services.

Attribution 1 Publication: MD AG's office / hhs.gov Author:
 Article Title: Middletown Medical PC
 Article URL: <http://www.recordonline.com/news/20180329/middletown-medical-dealing-with-data-breach>

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

Report Date: 7/2/2018

Page 81 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-22	inSite Digestive Health Care	CA	3/9/2018	Paper Data	Medical/Healthcare	Yes - Published #	1,424

inSite Digestive Health Care CA Healthcare Provider 1424 03/09/2018 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: inSite Digestive Health 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
ITRC20180401-21	West Creek Financial, Inc.	VA	3/22/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

This incident involved unauthorized persons potentially having access to your name, date of birth, address, the last four digits of your social security number, driver's license or government identification card number, telephone, bank account information, debit card information, and other identifying information ("Personal Information").

Attribution 1 Publication: NH AG's office / NY AG's office Author:
 Article Title: West Creek Financial, Inc.
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/west-creek-financial-20180322.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-20	Teal, Becker & Chiamonte, CPAs PC	NY	3/23/2018	Electronic	Business	Yes - Published #	5,576

To date, the investigations have revealed that a routine test was performed on November 29, 2017 on our data restoration procedures in an offsite, completely separate, cloud-based location maintained by a third party. The data at this separate location was the subject of a ransomware attack. The compromised data may have included personally identifiable information (PII) with some combination of your name, address, social security number and financial information. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office Author:
 Article Title: Teal, Becker & Chiamonte (CPAs)
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/teal-becker-20180323.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-19	Squire Patton Boggs	OH	3/26/2018	Electronic	Business	Yes - Published #	256

It has come to our attention that in the course of mailing out annual 1099s, a 1099 for one (1) individual recipient was mistakenly included in the envelope with another recipient's 1099. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: Squire Patton Boggs
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/squire-patton-20180326.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-18	NFP Property & Casualty Services, Inc.	NY	3/23/2018	Electronic	Business	Yes - Published #	573

On March 13, 2018, we learned that one of our employees received a phishing email that same day that was designed to appear as if it came from a company executive. Believing the email to be legitimate, the employee replied to the message and attached certain employees' 2017 IRS Form W-2s, which included your name, address, earnings information, and Social Security number. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: NFP Property & Casualty Services, Inc.
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/nfp-20180323.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-17	JC Penney Corporation, Inc.	TX	3/27/2018	Electronic	Business	Yes - Unknown #	Unknown

We recently became aware that a third-party vendor in possession of some of our supplier data experienced a security incident involving its Microsoft 365 environment between April and August 2017. The affected information may have included your name, address, Social Security number or employer identification number, if you provided such information to JCPenney in connection with your supplier documents.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
 Article Title: JC Penney Corporation, Inc.
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/jc-penney-20180327.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-16	Funding Circle USA, Inc. (Dun & Bradstreet, Inc.)	CA	3/23/2018	Electronic	Banking/Credit/Financial	Yes - Published #	10,796

Consistent with the requirements of N.H. Rev. Stat. §359-C:201(b), we are writing to inform you that Funding Circle USA, Inc. ("Funding Circle") was notified by Dun & Bradstreet, Inc. ("D&B"), one of Funding Circle's data vendors, on March 3, 2018 of a security incident involving certain of D&B's email accounts. D&B's investigation revealed that unauthorized third parties used compromised credentials to log into the email accounts of a limited number of D&B employees. This information included the names, addresses, phone numbers, and social security numbers of small business loan guarantors. (Exposure number per IN AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: Funding Circle USA, Inc. (Dun & Bradstreet, Inc.)
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/funding-circle-20180323.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-15	Northwest Asset Management (NWAM) dba RIA Innovations	WA	3/23/2018	Electronic	Banking/Credit/Financial	Yes - Published #	531

On January 31, 2018, we learned that an NWAM, LLC employee may have been the victim of an email phishing attack. The information that was available in the potentially compromised email account included your name and financial account number. (Exposure number per NC AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-14	ThermoFisher Scientific	MA	3/30/2018	Electronic	Business	Yes - Published #	2,900

Although the date when the compromise began has not been conclusively determined, our investigation to date confirms that certain emails from on or about July 6, 2017 through October 13, 2017 were acquired by unauthorized third parties. Based on our investigation to date, we believe that your name and social security number were among the information contained in the affected emails. (Exposure number per IN AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-13	Mintie Corporation	CA	3/27/2018	Electronic	Business	Yes - Published #	349

On February 16, 2018, we discovered that parts of our network were subject to a ransomware attack. The information may have included your credit card authorization form. This would involve your: name (or the business name if it was a business credit card), address attached to the credit card, credit card number, credit card verification value (CVV) and expiration date. (Exposure number per NC AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-12	Cambridge Health Alliance	MA	3/31/2018	Electronic	Medical/Healthcare	Yes - Published #	2,280

On January 31, 2018, the Everett Police Department (MA) informed CHA that patient information had been compromised and that three electronic files were found in the possession of an unauthorized third party. CHA immediately began our own investigation and determined that at least one of these files contained your healthcare billing information, which may have included your full name, address, phone number, date of birth, Social Security number, employer information, charges for past healthcare services, and discharge date.

Attribution 1 Publication: NH AG's office / pressherald.com / hhs.g Author:
Article Title: Data of 2,500 Massachusetts patients compromised
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/cambridge-health-20180328.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-11	CareFirst BlueCross BlueShield	MD	3/30/2018	Electronic	Medical/Healthcare	Yes - Published #	6,200

CareFirst BlueCross BlueShield said Friday it was hit by a phishing email attack that could have exposed the personal information of 6,800 of the insurer's members. The personal information that could have been compromised includes names, member identification numbers and date of birth. (Number of records exposed per hhs.gov)

Attribution 1 Publication: baltimoresun.com / hipaajournal.com / h Author:
Article Title: 6,800 affected in CareFirst phishing incident
Article URL: <http://www.baltimoresun.com/news/maryland/anne-arundel/bs-hs-carefirst-phishing-20180330-story.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-10	Under Armour / MyFitnessPal	MD	3/29/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 25, 2018, we became aware that during February of this year an unauthorized party acquired data associated with MyFitnessPal user accounts. The affected information included usernames, email addresses, and hashed passwords - the majority with the hashing function called bcrypt used to secure passwords. (Exposure number per <https://www.reuters.com/article/us-under-armour-databreach/under-armour-says-150-million-myfitnesspal-accounts-breached-idUSKBN1H532W>)

Attribution 1 Publication: MFP website, The Verge, CA AG's office Author:
Article Title: Under Armour / MyFitnessPal
Article URL: <https://content.myfitnesspal.com/security-information/notice.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-09	Mississippi State Department of Health	MS	3/26/2018	Electronic	Government/Military	Yes - Published #	30,799

Today letters were sent to Mississippi residents notifying that protected health information such as name, date of birth, social security number or lab results was accidentally released to J Michael Consulting, a contractor for the Centers for Disease Control and Prevention (CDC).

Attribution 1 Publication: MS State Department of Health website Author:
Article Title: Mississippi State Department of Health
Article URL: <https://msdh.ms.gov/msdhsite/ static/23.19687.341.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-08	Mendes & Haney, LLP	CA	3/29/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 21, 2018, the third-party forensic IT firm concluded their investigation and determined that there was unauthorized access to our network from a foreign IP address between January 23, 2018 and February 26, 2018 through Remote Desktop Protocol. If you are an individual, this information may have included your: name, birthdate, telephone number(s), address, Social Security number, employment (W-2) information, 1099 information (including account number if provided to us), and direct deposit bank account information (account number and routing information) if provided to us.

Attribution 1 Publication: CA AG's office / MT AG's office / MD AG Author:
Article Title: Mendes & Haney, LLP
Article URL: https://oag.ca.gov/system/files/M%26H%20notification_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-07	Applied Plan Administrators (a division of Retirement Advantage)	WI	3/28/2018	Electronic	Business	Yes - Published #	22,661

On February 23, 2018, the forensic firm determined that a third party gained unauthorized access to one APA employee's email account on February 10, 2018, using a phishing attack. The personally identifiable information potentially involved includes your name, address, Social Security number, financial institution information and other similar personal financial information. (Exposure number per IN AG's office)

Attribution 1

Publication: CA AG's office / MT AG's office / MD AG Author:

Article Title: Applied Plan Administrators (a division of Retirement Advantage)

Article URL: <https://oag.ca.gov/system/files/CORR%20A.%20Schlidt%20Letter%20to%20CA%20AG%20Data%20Incident%20Notifica>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-06	Fred Usinger, Inc.	WI	3/28/2018	Electronic	Business	Yes - Published #	35,147

On March 7, 2018, Fred Usinger, Inc.'s ("Usinger") hosting service provider for its e-commerce website informed Usinger that it had experienced a data security incident in which the personal information, including stored payment data, of a number of Usinger's customers appeared to have been accessed between the time period of September, 2017 and March, 2018. The unauthorized acquisition may have included personal information such as customer names, addresses, e-mail addresses, telephone numbers, credit or debit card numbers, and possibly your credit card security code. (Exposure number per IN AG's office)

Attribution 1

Publication: CA AG's office / MT AG's office Author:

Article Title: Fred Usinger, Inc.

Article URL: https://oag.ca.gov/system/files/Usinger%20Model%20Form%20of%20Notice%20of%20Data%20Breach%20Letter_1.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-05	Prudential Insurance Company of America	NJ	3/27/2018	Electronic	Business	Yes - Unknown #	Unknown

Prudential is the administrator of your <<ClientDef1(Company Name)>> variable annuity contract. An electronic file containing your personal information was inadvertently sent by a vendor of Prudential, to a corporate client of that vendor. The file contained your name, address, Social Security number, account number and financial information related to your annuity.

Attribution 1

Publication: CA AG's office Author:

Article Title: Prudential Insurance Company of America (11/2017)

Article URL: https://oag.ca.gov/system/files/Prudential%20template%20%28CA-63518%29_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-04	Paycor	OH	3/26/2018	Electronic	Business	Yes - Unknown #	Unknown

During the normal course of business, a Paycor employee accidentally mailed an encrypted computer disc ("CD") containing images of IRS W-2 tax information for you and fellow employees from Supreme Corporation and its affiliates. The CD was mailed directly to one recipient at another trusted Paycor client company.

Attribution 1

Publication: CA AG's office Author:

Article Title: Paycor

Article URL: https://oag.ca.gov/system/files/Supreme%20Corporation%20Notice%20Letter%20-%20CA_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-03	Branton, de Jong & Associates	CA	3/25/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 16, 2018, the specialized forensic IT firm determined that there was unauthorized access to our system from a foreign IP address. The information may have included your full name, birthdate, telephone number, address, Social Security number, all employment (W-2) and self-employment information, 1099 information, entity identification and income earned/amounts received from participation in S-Corp/partnership/LLC/trust, and direct deposit bank account information if provided to us (which includes account number and routing information).

Attribution 1

Publication: CA AG's office / MT AG's office / MD AG Author:

Article Title: Branton, de Jong & Associates

Article URL: https://oag.ca.gov/system/files/Branton%20Notice_0.pdf

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

Report Date: 7/2/2018

Page 85 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-02	S.O.S. Tax	CA	3/22/2018	Electronic	Business	Yes - Unknown #	Unknown

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a security data breach incident that may involve your personal information between October 2017 and March 2018. The data accessed may have included but not limited to personal information such as names, dates of birth, social security numbers, and emails.

Attribution 1 Publication: CA AG's office Author:
 Article Title: S.O.S. Tax
 Article URL: https://oag.ca.gov/system/files/SOS001%20Letter%20of%20Security%20Data%20Breach_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180401-01	Shutterfly (Workday)	CA	3/28/2018	Electronic	Business	Yes - Published #	9,428

On March 20, 2018, we learned that a Shutterfly employee's credentials were used without authorization to access our Workday test environment on January 11, 2018. As such, potentially exposed data may have included items such as your name, social security number, date of birth, and work email; any passport number, state ID (including driver's license), bank account and routing numbers, pay stub information, or personal email that was on file in Workday; and the names, dates of birth, and social security numbers of any beneficiaries and/or dependents that were on file in Workday. (Exposure number per IN AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office Author:
 Article Title: Shutterfly
 Article URL: https://oag.ca.gov/system/files/ADULT%20Letter_EE_Contractor_Dependent_Beneficiary_vFinal_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180327-01	Bronson Laboratories / Bronson Nutritionals	MI	3/19/2018	Electronic	Medical/Healthcare	Yes - Published #	25,450

We recently identified malware on certain of our systems. We believe the malware was designed to collect customers payment card information, including cardholder name and address, payment card number, security code and expiration date. (Exposure number per NC AG's office)

Attribution 1 Publication: CA AG's office / MD AG's office Author:
 Article Title: Bronson Laboratories / Bronson Nutritionals
 Article URL: <https://oag.ca.gov/system/files/Bronson%20Nutritionals%20-%20Template%20Individual%20Notification%20Letter%20>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180326-05	GY Agemni	UT	3/16/2018	Electronic	Business	Yes - Published #	320

On January 18, 2018, we learned that a single authorized user of our software system used customer information to make improper charges for his personal benefit. Our investigation revealed that your information, which included your name, address, and credit card number, was not disclosed to any other individuals, and that this person no longer has access to your personal information. (Exposure number per IN AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180326-04	Oregon Department of Revenue	OR	3/23/2018	Electronic	Government/Military	Yes - Published #	36,000

An employee at Oregon's tax collection agency copied the data of 36,000 people, including social security numbers, and stored the files to a personal account, the state announced on Friday.

Attribution 1 Publication: oregonlive.com / OR AG's office Author:
 Article Title: Oregon tax agency employee copied personal data of 36,000 people
 Article URL: http://www.oregonlive.com/politics/index.ssf/2018/03/oregon_tax_agency_employee_cop.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180326-03	Marquis ID Systems	HI	3/23/2018	Electronic	Business	Yes - Published #	66,500

Marquis ID Systems, which issues state driver's licenses and ID cards, reported Thursday that a system crash in September resulted in the loss of scans of sensitive personal documents that might prove irretrievable.

Attribution 1	Publication: hawaiitribune-herald.com	Author:					
	Article Title: License, ID data lost in crash: System failure affects 9,193 Hawaii Island residents						
	Article URL: http://www.hawaiitribune-herald.com/2018/03/23/hawaii-news/license-id-data-lost-in-crash-system-failure-affects-9193-						

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180326-01	King & Associates, CPA	PA	3/23/2018	Electronic	Business	Yes - Published #	2,009

While the investigation is ongoing, we determined there was unauthorized access to a tax program utilized by our company containing information on our clients and their dependents. The tax program stored the following categories: name, address, Social Security number, Driver's License number, date of birth, and in some cases, bank account information if used to pay taxes due or have refunds sent to your bank account. (Exposure number per NC AG's office)

Attribution 1	Publication: MT AG's office	Author:					
	Article Title: King & Associates, CPA						
	Article URL: https://dojmt.gov/wp-content/uploads/King-Associates-CPA-P.C..pdf						

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180323-04	UnitedHealth Group Single Affiliated Covered Entity	MN	3/15/2018	Paper Data	Medical/Healthcare	Yes - Published #	1,755

UnitedHealth Group Single Affiliated Covered Entity MN Health Plan 1755 03/15/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1	Publication: hhs.gov	Author:					
	Article Title: UnitedHealth Group Single Affiliated Covered Entity						
	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
ITRC20180323-03	Arc of Erie County	NY	3/9/2018	Electronic	Medical/Healthcare	Yes - Published #	3,751

Between July 2015 and February 2018, the two spreadsheets could be accessed over the Internet by unauthorized individuals as a result of a coding error on the website. The coding error saw a link included on the website that allowed the spreadsheets to be accessed. The Arc spreadsheets contained sensitive information such as names, Social Security numbers and diagnosis codes.

Attribution 1	Publication: hhs.gov / hipaajournal.com	Author:					
	Article Title: 3,751 Patients' PHI Exposed on Internet for More Than 30 Months						
	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
ITRC20180323-02	North Texas Medical Center	TX	3/15/2018	Electronic	Medical/Healthcare	Yes - Published #	3,350

On February 26, 2018, NTMC discovered that an individual viewed an e-mail containing a spreadsheet with a resident's information, which was inadvertently provided in response to a Public Information Act request made under Chapter 552 of the Texas Government Code. The spreadsheet contained the resident's name, Social Security Number, date of birth, admission date, discharge date, and the abbreviation of the department where the services occurred.

Attribution 1	Publication: NH AG's office / hhs.gov	Author:					
	Article Title: North Texas 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
ITRC20180323-01	City of Atlanta	GA	3/23/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

The source of the problem: a ransomware attack that had compromised multiple systems. The malware's impact is still being assessed. City of Atlanta IT staff are working with investigators from the FBI, Department of Homeland Security, Microsoft and Cisco to determine what data has been encrypted. Type of information exposed was not disclosed.

Attribution 1 Publication: forbes.com Author:
Article Title: City Of Atlanta Computers Hit By Ransomware Attack
Article URL: <https://www.forbes.com/sites/leemathews/2018/03/23/city-of-atlanta-computers-hit-by-ransomware-attack/-11fd06172>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180322-06	John J. Pershing VA Medical Center	MO	3/7/2018	Paper Data	Government/Military	Yes - Published #	1,843

John J. Pershing VA Medical Center MO Healthcare Provider 1843 03/07/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: John J. Pershing VA 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
ITRC20180322-05	Saint Francis Hospital	GA	3/14/2018	Electronic	Medical/Healthcare	Yes - Published #	1,412

Saint Francis Hospital GA Healthcare Provider 1412 03/14/2018 Improper Disposal Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Saint Francis 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
ITRC20180322-04	CareMeridian, LLC (Bullpen Financial, Inc.)	CA	3/22/2018	Electronic	Medical/Healthcare	Yes - Published #	1,922

On December 21, 2017, CareMeridian discovered that an unencrypted disk sent by a third-party software provider containing documents that included sensitive information appeared to have been lost in the mail. It was determined that with respect to CareMeridian the lost disk contained one or more of the following types of information: name and limited medical information, and, for 13 individuals, social security number.

Attribution 1 Publication: Company press release / CA AG's office Author:
Article Title: CareMeridian, LLC
Article URL: <https://www.businesswire.com/news/home/20180321006190/en/CareMeridian-LLC-Issues-Data-Breach-Notice>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180322-03	National Mentor Healthcare, LLC dba Georgia MENTOR (Bullpen Financial, Inc.)	GA	3/21/2018	Electronic	Medical/Healthcare	Yes - Published #	1,015

On December 21, 2017, Georgia MENTOR discovered that an unencrypted disk sent by a third-party software provider containing documents that included sensitive information appeared to have been lost in the mail. It was determined that with respect to Georgia MENTOR the lost disk contained one or more of the following types of information: name and limited medical information, and, for one individual, social security number.

Attribution 1 Publication: Company press release / hhs.gov Author:
Article Title: Georgia MENTOR Issues Data Breach Notice
Article URL: <https://www.businesswire.com/news/home/20180321006192/en/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180322-02	Community First Bank	WI	3/20/2018	Electronic	Banking/Credit/Financial	Yes - Published #	2,837

On March 2, 2018, we learned that certain personal information could have been viewed as part of an email account compromise. You are receiving this notice because certain of your personal information was in the account and could have been accessed, including your name, date of birth, address, Social Security number and, for some individuals, driver's license number. (Exposure number per IN AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180321-04	Klamath County Falls	OR	3/20/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

An employee's network credentials were compromised by a phishing scam email apparently originating in Nigeria, according to Morris. The scam succeeded in forwarding all of the employee's incoming emails to another email account. Type of information exposed was not disclosed.

Attribution 1 Publication: Klamath County Press Release Author:
Article Title: KLAMATH COUNTY FALLS PREY TO ELECTRONIC SECURITY BREACH
Article URL: <https://static1.squarespace.com/static/59b9f24c64b05fd6531db026/t/5ab1eaa00e2e72081e61de69/1521609376406/03-20>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180321-03	Special Agents Mutual Benefit Association	MD	3/13/2018	Paper Data	Business	Yes - Published #	13,942

During the mailing preparation process, a programming error occurred whereby some subscribers received a Form 1095-B containing the name and Social Security number for one or more family members of another plan subscriber.

Attribution 1 Publication: hhs.gov / SAMBA press release Author:
Article Title: Special Agents Mutual Benefit Association (SAMBA)
Article URL: <https://www.prnewswire.com/news-releases/samba-provides-notice-of-data-incident-300618553.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180321-02	Food Industry Self Insurance Fund of New Mexico / Adjusting Alternatives, LLC	NM	3/8/2018	Electronic	Business	Yes - Unknown #	Unknown

On February 7, 2018, the U.S. Postal Service and a USPS Inspector confirmed that an unidentified thief broke into a USPS mailbox and stole the bin, which contained your benefit check. We immediately contacted our financial institution to stop payment on the checks, and have since reissued and re-sent the checks. Unfortunately, the checks contained your name, address, and Social Security number.

Attribution 1 Publication: MT AG's office Author:
Article Title: Food Industry Self Insurance Fund of New Mexico
Article URL: <https://dojmt.gov/wp-content/uploads/Food-Industry-Self-Insurance-Fund.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180321-01	Island Outdoor, LLC	NY	3/15/2018	Electronic	Business	Yes - Published #	979

On February 23, 2018, we discovered that we were the victims of a sophisticated cyber-attack that resulted in the potential compromise of some customers' debit and credit card data used at www.BBQgaskets.com, www.BBQsmokerSupply.com, www.StoveGaskets.com, www.WholesaleSmokerParts.com, and www.UDSparts.com between November 1, 2017 and January 31, 2018 and February 9, 2018 and February 14, 2018. (Exposure number per NC AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180320-06	Orbitz (Expedia subsidiary)	IL	3/19/2018	Electronic	Business	Yes - Published #	880,000

While conducting an investigation of a legacy Orbitz travel booking platform (the "platform"), we determined on March 1, 2018 that there was evidence suggesting that, between October 1, 2017 and December 22, 2017, an attacker may have accessed personal information, stored on this consumer and business partner platform, that was submitted for certain purchases made between January 1, 2016 and June 22, 2016. On March 1, 2018, we determined that the personal information that was likely accessed may have included your full name, payment card information, date of birth, phone number, email address, physical and/or billing address, and gender.

Attribution 1 Publication: securityblvd.com / MT AG's office Author:
Article Title: Orbitz Discloses Possible Data Breach Affecting 880,000 Payment Cards
Article URL: <https://dojmt.gov/wp-content/uploads/Orbitz-3-27-18.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180320-05	Skamania Public Utility District	WA	3/16/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 17, 2018, Skamania PUD discovered that an unauthorized person gained access to the email account of a Skamania PUD employee. We conducted a thorough review of the employee's email account and determined, on March 9, 2018, that the unauthorized person had access to an email message or attachment in the employee's email account that contained your name and <<variable data field>>. Type of information exposed was not disclosed.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180320-04	Clarfield Financial Advisors (Schwab Advisor Center)	NY	3/9/2018	Electronic	Banking/Credit/Financial	Yes - Published #	1,178

On March 9, 2018, CFA learned from Schwab that an unknown person or persons gained access to the Schwab Advisor Center website using CFA credentials. This website is used by CFA to manage your account at Schwab. The information acquired included your name, Social Security number, address, and Schwab account number. (Exposure number per NC AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Clarfield Financial Advisors (Schwab Advisor Center)
Article URL: <https://dojmt.gov/wp-content/uploads/Clarfield-Financial-Advisors.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180320-03	Invacare Corporation	OH	3/14/2018	Electronic	Medical/Healthcare	Yes - Published #	187

On February 16, 2018, Invacare Corporation discovered that an unauthorized third party obtained access to an Invacare employee's email account starting on or about January 1, 2018. Based on our investigation, your name, address, and Social Security Number or Taxpayer Identification Number were impacted. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Invacare Corporation
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/invacare-20180314.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180320-02	ISS Solutions / Geisinger Health	PA	3/6/2018	Electronic	Medical/Healthcare	Yes - Published #	2,295

On January 23, 2018, ISS, a Geisinger company, was the victim of a ransomware attack. We concluded that the following personal data regarding you may have been present on the affected drive:
Your name, address, phone number, social security number, birth date, email address. The name, address, phone number, social security number and date of birth of any dependents on your insurance.
Copies of documents used to support employee eligibility to work in the United States. These documents may have included: your passport, permanent resident card, state or federal id card, driver's license, social security card, and/or birth certificate. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office / hhs.gov Author:
Article Title: ISS Solutions
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/iss-20180306.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180320-01	Serene Sedation	MD	3/14/2018	Electronic	Medical/Healthcare	Yes - Published #	5,207

This notification is to inform you that data belonging to Serene Sedation, LLC (Serene) an authorized Business Associate, also had financial data on the same system that could have been accessed in that cyber-attack. The data elements involved may have included name, medical diagnosis, a Serene invoice tracking number, and location of service provided.

Attribution 1 Publication: MD AG's office / hhs.gov Author:
Article Title: Serene Sedation
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295275.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180319-04	Frost Bank	TX	3/17/2018	Electronic	Banking/Credit/Financial	Yes - Published #	470

The San Antonio based-bank issued a statement that said Frost detected the unauthorized access to a third-party lockbox software program earlier this week and immediately launched an investigation. The software allowed unauthorized users to view and copy images of checks stored electronically.

Attribution 1 Publication: ksat.com / databreaches.net Author:
Article Title: SA-based Frost Bank investigating breach, contacting affected customers
Article URL: <https://www.ksat.com/news/sa-based-frost-bank-investigating-breach-contacting-affected-customers>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180319-03	Holiday Inn Sacramento / Atrium Hospitality	GA	3/17/2018	Electronic	Business	Yes - Published #	182

On December 8, 2017, Atrium Hospitality discovered that a workstation at the Holiday Inn Sacramento was potentially impacted by ransomware. On February 14, 2018, Atrium Hospitality determined that one or more of the following for three hundred and seventy-six (376) hotel guests was potentially accessible: name, driver's license number, passport number, and credit or debit card information. (Exposure number per IN AG's office)

Attribution 1 Publication: Atrium Press Release / VT AG's office / Author:
Article Title: Atrium Hospitality Notifies Hotel Guests of Compromise
Article URL: <https://www.prnewswire.com/news-releases/atrium-hospitality-notifies-hotel-guests-of-compromise-300615517.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180319-02	Primary Health Care, Inc.	IA	3/18/2018	Electronic	Medical/Healthcare	Yes - Published #	10,313

On March 1, 2017, PHC discovered that the email accounts of four of its employees had been subject to unauthorized access on February 28, 2017. The patient information located in one of the email accounts or Google drives and therefore potentially subject to unauthorized access includes a combination of patient name, phone number, Social Security number, driver's license number, financial account number, credit/debit card number, date of service, diagnosis and treatment information, medical history, facility and provider visited, health insurance/payor information and, if applicable, Medicaid identification number.

Attribution 1 Publication: PHC website Author:
Article Title: Multiple Email Accounts Compromised at Primary Health Care
Article URL: <http://www.phciowa.org/call-center/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180319-01	Taylor-Dunn Manufacturing Company	CA	1/24/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 24, 2018, we identified unauthorized access in the form of cryptomining malware on the server that contains our online customer care and dealer centers at <https://www.taylor-dunn.com>. The file that was accessed includes name, address, phone number, email address, and your customer care or dealer center username and password.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Taylor-Dunn Manufacturing Company
 Article URL: https://oag.ca.gov/system/files/Taylor-Dunn_CA_Notice_Sample_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180316-04	Swenson, Saurer, Gerber, Anderson & Co., Ltd.	MN	3/6/2018	Electronic	Business	Yes - Published #	1,664

In February, 2018, our Firm became aware that an unauthorized third party may have gained access to your 2015 tax information, including your first and last name, address, Social Security number ("SSN") and compensation information as well as possibly your bank account information if direct deposit/direct payment was utilized. (Exposure number per IN AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
 Article Title: Swenson, Saurer, Gerber, Anderson & Co., Ltd.
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/swenson-saurer-20180306.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180316-03	Laufer Group International	NY	2/27/2018	Electronic	Business	Yes - Unknown #	Unknown

On February 16, 2018, an email that purportedly was sent from Mr. Mark Laufer (Laufer Group's chief executive officer) requested that the recipient (an employee of Laufer Group) provide him the 2017 W-2 forms for employees who were employed by the company last year, via a reply email.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
 Article Title: Laufer Group International
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/laufer-20180227.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180316-02	ICF	VA	3/2/2018	Electronic	Business	Yes - Published #	900

An authorized ICF employee accidentally e-mailed a file with W-2 statements for approximately 900 current and former ICF employees to a current ICF employee email account (ICF Recipient). This email was not encrypted or password protected, and the ICF Recipient was an unauthorized recipient. The ICF Recipient was sent not only their own W-2 statement, but others as well.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
 Article Title: ICF
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/icf-20180302.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180316-01	Nampa School District	ID	3/15/2018	Electronic	Educational	Yes - Published #	4,054

We recently learned that an individual gained unauthorized access to a school district email account, which contained information about a limited number of employees. The information stored in the affected email account includes certain individuals' names, Social Security numbers, birthdates, and/or financial information. (Exposure number per NY AG's office)

Attribution 1 Publication: kivitv.com / MT AG's office / NY AG's office Author:
 Article Title: Nampa School District investigating cyber security breach
 Article URL: <https://dojmt.gov/wp-content/uploads/Nampa-School-District-1.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180315-02	Dover Business Services	TX	3/9/2018	Electronic	Business	Yes - Unknown #	Unknown

On March 2, 2018, we learned that the USB drive was lost or destroyed in transit to DAL and that the USB drive was not encrypted or password-protected. These files included your name, address, Social Security number, income and withholding information and in some cases, garnishment information. In some specific cases, the information lost also included bank account information, but not bank account passcodes or access codes.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180315-01	MBM Company Inc. (Custom Personalization Solutions, LLC dba Iimages Jewelry)	AR	3/14/2018	Electronic	Business	Yes - Unknown #	Unknown

On February 6th, 2018 researchers at Kromtech security came across another publicly accessible Amazon s3 bucket. This one contained a MSSQL database backup, which was found to hold the personal information, including names, addresses, zip codes, phone numbers, e-mail addresses, ip addresses, and, most shockingly, plain text passwords, for shopping accounts of over 1.3 million people (1,314,193 to be exact) throughout the US and Canada.

Attribution 1 Publication: mackeepersecurity.com / VT AG's office Author:
Article Title: MSSQL database containing the personal information of approximately 1.3 million people found in another public Amazon S3
Article URL: <https://mackeepersecurity.com/post/walmart-jewelry-partner-exposed-millions-customer-details>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180314-04	Travel Corporation	CA	3/9/2018	Electronic	Business	Yes - Unknown #	Unknown

Yesterday afternoon, February 26, 2018, our Director of Human Resources received an e-mail from what appeared to be our Global Chief Executive Officer, requesting certain payroll information and copies of 2017 W2s for all of our employees located in the United States. Names, addresses, Social Security numbers, and W2s of all present USA employees and a number of former USA employees.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180314-03	Port of Longview	WA	3/13/2018	Electronic	Business	Yes - Published #	370

The Port of Longview was recently victimized by a cyber attack that may have affected hundreds of past and current employees and dozens of vendors. The investigation was able to confirm that two administrator accounts were hacked. Type of information exposed was not disclosed.

Attribution 1 Publication: tdn.com / databreaches.net Author:
Article Title: Port of Longview hit with major cyberattack
Article URL: http://tdn.com/news/local/port-of-longview-hit-with-major-cyberattack/article_25102b63-d897-5cfd-b16b-ffec70545d1d.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180314-02	QuadMed LLC (Hillenbrand Inc. Occupational Health and Stoughton Trailers)	WI	2/26/2018	Electronic	Medical/Healthcare	Yes - Published #	5,305

QuadMed, a Wisconsin-based provider of medical, laboratory, pharmacy, fitness, and physical therapy services, has discovered the protected health information of 5,305 patients has potentially been impermissibly disclosed to certain employees. The types of protected health information that could potentially have been accessed included patients' names, onsite clinic service dates, test and evaluation results, diagnoses, medical histories, information on examinations and physicals, vaccinations, travel medicine prescriptions, and workers' compensation data.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: QuadMed Discovers PHI of More than 5,300 Patients Was Impermissibly Disclosed to Employees
Article URL: <https://www.hipaajournal.com/quadmed-phi-5300-patients-impermissibly-disclosed/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180314-01	Interstate Plastics, Inc.	CA	3/6/2018	Electronic	Business	Yes - Published #	1,031

On or around December 23, 2017, we learned of suspicious activity related to our e-commerce website. We immediately commenced an investigation and determined that our e-commerce site was infected with a suspicious code. The investigation has confirmed the following information could be collected by the malicious code: name, address, card number, expiration date, and CVV. (Exposure number per NC AG's office)

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: Interstate Plastics, Inc.
Article URL: <https://dojmt.gov/wp-content/uploads/Interstate-Plastics-2nd-notice.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180313-09	Okaloosa County Water and Sewer	FL	3/12/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

There may have been a security break for Okaloosa County Water and Sewer users who paid their bills with a credit or debit card, according to a press release from the county. The reports have raised a concern that the online payment system may have been breached.

Attribution 1 Publication: nwfailynews.com Author:
Article Title: Okaloosa Water and Sewer warns users of possible security breach
Article URL: <http://www.nwfailynews.com/news/20180312/okaloosa-water-and-sewer-warns-users-of-possible-security-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180313-08	University of Pennsylvania (PENN)	PA	3/12/2018	Electronic	Educational	Yes - Published #	9,000

The email indicates that advance class registration lists for this past spring semester were downloaded by an unauthorized user, who accessed the lists through a "course registration application." That server has since been taken offline. The class lists contained information on class enrollment and included students' name and the last four digits of their social security numbers, according to the email sent out this afternoon by Chief University Privacy Officer Scott Schafer.

Attribution 1 Publication: Daily Pennsylvanian Author:
Article Title: Approx. 9,000 Penn students affected by security breach that released their private information
Article URL: <http://www.thedp.com/article/2018/03/privacy-breach-student-information-upenn-penn-philadelphia-class-lists-registra>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180313-07	South Carolina Commission on Higher Education	SC	3/12/2018	Electronic	Educational	Yes - Published #	3,000

About 3,000 South Carolina college scholarship recipients had their personal information exposed online for nearly a year, state regulators revealed Monday.

Attribution 1 Publication: postandcourier.com Author:
Article Title: Personal data of 3,000 South Carolina college scholarship recipients exposed for nearly a year
Article URL: <https://www.postandcourier.com/politics/personal-data-of-south-carolina-college-scholarship-recipients-exposed-for/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180313-06	ATI Holdings, LLC	IL	3/13/2018	Electronic	Medical/Healthcare	Yes - Published #	34,665

As part of this investigation, ATI recently determined that certain ATI employee email accounts were accessed without authorization between January 9, 2018 and January 12, 2018, and that certain types of patient information were included within one or more of these email accounts. Affected email accounts contained, and the unauthorized actor may have had access to, information related to certain ATI patients, including the following types of information: name, date of birth, driver's license or state identification number, Social Security number, credit card number, financial account number, patient identification number...and more PHI (Exposure number per IN AG's office)

Attribution 1 Publication: ATI website / MT AG's office / hhs.gov Author:
Article Title: ATI Holdings, LLC
Article URL: <https://news.atipt.com/data-privacy-event-update/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180313-05	Curtin Maritime Corp.	CA	3/5/2018	Electronic	Business	Yes - Published #	191

On January 23, 2018, we discovered that on January 22, 2018, certain personnel information was acquired without authorization. The incident may have involved passports, driver's licenses, and Social Security numbers. (Exposure number per IN AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180313-03	CNU Online Holdings, LLC dba Net Credit	IL	3/8/2018	Electronic	Banking/Credit/Financial	Yes - Published #	3,011

On or about February 20, 2018, our security team discovered that an unauthorized party used valid email addresses and passwords to log in to a small percentage of NetCredit accounts. Access to an account could have enabled the unauthorized party to view the account holder's name, telephone number, physical address, last four digits of their bank account number, NetCredit account number, last four digits of their Social Security number, and basic employment and income information. (Exposure number per NC AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office Author:
Article Title: CNU Online Holdings, LLC dba Net Credit
Article URL: <https://dojmt.gov/wp-content/uploads/CNU-Online-Holdings-LLC-NetCredit.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180313-02	Barnes-Jewish Healthcare	MO	3/13/2018	Electronic	Medical/Healthcare	Yes - Published #	33,482

The protected health information of 33,420 patients of BJC Healthcare has been accessible on the Internet for eight months without any need for authentication to view the information.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: PHI of 33,420 BJC Healthcare Patients Exposed on Internet for 8 Months
Article URL: <https://www.hipaajournal.com/phi-of-33420-bjc-healthcare-patients-exposed-on-internet-for-8-months/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180313-01	Neil D. DiLorenzo CPA, P.C.	CO	3/9/2018	Electronic	Business	Yes - Published #	963

Our investigation determined that on January 13, 2018, an unauthorized third party had accessed a computer system that contained files related to tax returns and may have contained your name, address, Social Security number, wage information and bank account information if you provided it to us. (Exposure number per NC AG's office)

Attribution 1 Publication: MT AG's office / NY AG's office / NC AG' Author:
Article Title: Neil D. DiLorenzo CPA, P.C.
Article URL: <https://dojmt.gov/wp-content/uploads/DiLorenzo-CPA.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180312-03	Harper's Magazine	NY	2/22/2018	Electronic	Business	Yes - Unknown #	Unknown

Harper's Magazine, the monthly longform journalism and essay publication, has warned subscribers that their passwords may have been stolen by hackers. On Thursday several subscribers tweeted screenshots of an email that Harper's sent. "It has come to our attention that your username and password for Harpers.org may have been compromised," the email reads.

Attribution 1 Publication: motherboard.vice.com Author:
Article Title: Harper's Magazine Warns Subscribers That Passwords May Have Been Stolen
Article URL: https://motherboard.vice.com/en_us/article/pammz9/harpers-magazine-warns-subscribers-that-passwords-may-have-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180312-02	Chopra Enterprises, LLC	CA	3/7/2018	Electronic	Business	Yes - Published #	614

The preliminary findings of the digital forensics investigation confirmed that your payment card information may have been acquired without authorization. Payment cards used by customers on Chopra's e-commerce website may have been involved in this data security incident. The affected payment card information may have included names, card numbers, expiration dates, and security codes. (Exposure number per NC AG's office)



Attribution 1 Publication: NH AG's office / MT AG's office / NY AG' Author:
 Article Title: Chopra Enterprises, LLC
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/chopra-20180307.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180312-01	Florida Virtual School	FL	3/9/2018	Electronic	Educational	Yes - Published #	368,000

FLVS learned that unauthorized individuals appear to have gained access to some of our computer systems that stored personal information relating to certain students, parents of students, and Leon County Schools' teachers.

Attribution 1 Publication: FLVLS.net notice Author:
 Article Title: Florida Virtual School (FLVS) / Leon County Schools
 Article URL: <https://www.flvs.net/notice>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180309-01	Insight Sourcing Group Holdings	GA	1/23/2018	Electronic	Business	Yes - Published #	123

We recently learned that a limited number of email users within Insight Sourcing Group & SpendHQ were victims of a criminal phishing attack resulting in unauthorized access to those users' email boxes from approximately November 30, 2017 through December 11, 2017. Although the comprehensive forensic investigation is ongoing, we believe that an unauthorized third party may have had access to an email containing names, addresses, date of births, and Social Security numbers. (Exposure number per IN AG's office)

Attribution 1 Publication: WA AG's office Author:
 Article Title: Insight Sourcing Group Holdings
 Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Safeguarding_Consumers/Breach%20InsightSour

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180308-03	Centris Federal Credit Union	NE	3/1/2018	Electronic	Banking/Credit/Financial	Yes - Published #	12,049

On January 15, 2018, the United States Secret Service provided two files to Centris. One of those files contained seven tables, two of which contain Centris data related to new account applications and consumer loan applications. Specifically, those two files contain individuals' names and, in certain circumstances, Social Security numbers and/or driver's license numbers. The Secret Service has not been able to provide further information on where it obtained the files due to its ongoing investigation. (Exposure number per NC AG's office)

Attribution 1 Publication: IA AG's office / MT AG's office Author:
 Article Title: Centris Federal Credit Union
 Article URL: https://www.iowaattorneygeneral.gov/media/cms/030118_Centris_Federal_Credit_Union_C682106B3D20B.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180308-02	Mize Houser & Company, P.A.	KS	2/23/2018	Electronic	Business	Yes - Unknown #	Unknown

In early February, we learned that your W2 may have been damaged during the mailing process which may have allowed personal information to be viewable. The information that was contained in the 2017 W2 that may have been damaged included your name, address, tax and earnings information, and Social Security number.

Attribution 1 Publication: IA AG's office Author:
 Article Title: Mize Houser & Company, P.A.
 Article URL: https://www.iowaattorneygeneral.gov/media/cms/022318_Mize_Houser_Company_P_41C8BE8226FA6.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180308-01	Front Range Dermatology Associates	CO	3/8/2018	Electronic	Medical/Healthcare	Yes - Published #	1,070

The breach occurred when a Front Range employee gave the data to a former employee. The compromised data includes patients' names, medical record numbers, dates of service, billing codes, names of insurance companies and dates and amounts of payments.



Attribution 1 Publication: hhs.gov / greeleytribune.com Author:
 Article Title: Front Range Dermatology Associates suffers a breach of medical records
 Article URL: <https://www.greeleytribune.com/news/news-briefs/front-range-dermatology-associates-suffers-a-breach-of-medical-re>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180307-08	GreyHealth Group	NY	3/1/2018	Electronic	Business	Yes - Published #	683

We regret to inform you that ghg / GreyHealth Group was recently targeted in a phishing scam that resulted in an unauthorized party obtaining some of your personal information. The records were 2017 W2 tax forms which contained your name, home address, social security number and salary information. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office / NC AG's office / NY AG' Author:
 Article Title: GreyHealth Group
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/greyhealth-20180301.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180307-07	ABC Bus Companies	MN	3/2/2018	Electronic	Business	Yes - Published #	741

On February 16, 2018, a phishing email was sent to an employee of ABC requesting the production of all employee W-2s for 2017. Thinking it was an official communication, the ABC employee responded by sending three (3) emails with various documents containing the following personal information of ABC employees: first and last name, address, date of birth, and Social Security number. In some instances, actual W-2 forms were also produced. (Exposure number per IN AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: ABC Bus Companies
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/abc-bus-20180302.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180307-06	California State University - Fresno	CA	3/6/2018	Electronic	Educational	Yes - Published #	10,777

The theft of an external hard drive at Fresno State could expose the personal data of at least 15,000 people. The hard drive was reported missing Jan. 12 and Fresno State officials said some of the files may have contained personal information, including names, addresses, phone numbers, birth dates, credit card numbers, driver's license numbers and full or last four digits of Social Security numbers. (Exposure number per IN and NC AG's office)

Attribution 1 Publication: govtech.com / databreaches.net / NH A Author:
 Article Title: Stolen University Hard Drive Potentially Exposes Thousands of Records
 Article URL: <http://www.govtech.com/security/Stolen-University-Hard-Drive-Potentially-Exposes-Thousands-of-Records.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180307-05	Rhode Island Executive Office of Health and Human Services 1095B	RI	2/27/2018	Paper Data	Government/Military	Yes - Published #	1,100

Rhode Island Executive Office of Health and Human Services 1095B RI Health Plan 1100 02/27/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: Rhode Island Executive Office of Health and Human Services 1095B
 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
ITRC20180307-04	Rhode Island Executive Office of Health and Human Services SNAP	RI	2/27/2018	Electronic	Government/Military	Yes - Published #	5,600

Rhode Island Executive Office of Health and Human Services SNAP RI Health Plan 5600 02/27/2018 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
 Article Title: Rhode Island Executive Office of Health and Human Services SNAP
 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
ITRC20180307-03	ConnectiCare	CT	2/21/2018	Paper Data	Medical/Healthcare	Yes - Published #	1,834

ConnectiCare CT Health Plan 1834 02/21/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: ConnectiCare
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
ITRC20180307-02	Center for Sports Medicine and Orthopedics	TN	2/26/2018	Paper Data	Medical/Healthcare	Yes - Published #	800

Center for Sports Medicine and Orthopedics TN Healthcare Provider 800 02/26/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Center for Sports Medicine and Orthopedics
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
ITRC20180307-01	Mercy Health Love County Hospital and Clinic	OK	2/26/2018	Electronic	Medical/Healthcare	Yes - Published #	14,229

On December 27, 2017, when performing a computer inventory, Mercy Health Love County Hospital and Clinic ("Love County Hospital") discovered that it was unable to locate documentation confirming the destruction of several older desktop computers no longer in use. Because you received services from Love County Hospital, we are providing you with this notice out of an abundance of caution, in the event that the computers may have contained your name, address or other demographic, clinical or billing information. (Exposure number per NC AG's office)

Attribution 1 Publication: VT AG's office / hhs.gov Author:
Article Title: Mercy Health Love County Hospital
Article URL: <http://ago.vermont.gov/blog/2018/02/27/mercy-love-county-hospital-clinic-sbn-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-19	Coastal Cape Fear Eye Associates	NC	2/14/2018	Electronic	Medical/Healthcare	Yes - Published #	925

On December 5, 2017, we discovered that, despite the security measures put in place by us and our information technology consultant, a file on CCFEA's computer system was infiltrated by ransomware. The ransomware attack did result in a compromising of certain electronic files containing patient records including patient names, addresses, dates of birth, phone numbers, Social Security Numbers, insurance card numbers, driver's license numbers, email addresses, ethnicities, emergency contacts, medical histories, medications, legal documents, diagnosis records, physician notes, medical diagrams, and billing and payment histories, as well as scanned copies of Medicare cards, insurance cards, and drivers' licenses.

Attribution 1 Publication: hipaajournal.com / hhs.gov / MD AG's of Author:
Article Title: Coastal Cape Fear Eye Associates
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295071%20\(2\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295071%20(2).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-17	Massachusetts Mutual Life Insurance Company	MA	2/16/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 30, 2018 MassMutual's Security Operations Center identified a configuration issue with a software tool used by a limited number of MassMutual associates. Your personal information that may have been involved includes your [name], [policy number], [address], [date of birth], [agent identification number], [last four digits of your Social Security number], [full Social Security number] .

Attribution 1 Publication: NH AG's office Author:
Article Title: Massachusetts Mutual Life Insurance Company
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/massachusetts-mutual-20180216.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-16	Beachbody, LLC	CA	3/1/2018	Electronic	Business	Yes - Published #	920

On February 2, 2018, we learned that some of our Coaches received the wrong IRS Form 1099-MISC (1099). We immediately investigated the incident and discovered that due to an error, a small number of the 1099s were mis-mailed, and went to an incorrect Coach. The information in your 1099 included your first name, last name, and only the last four digits of your social security number. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office Author:
Article Title: Beachbody, LLC
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/beachbody-20180301.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-15	Autoliv ASP, Inc.	MI	2/16/2018	Electronic	Business	Yes - Published #	114

On January 24, 2018, an email attaching a spreadsheet that contained 114 employees' social security numbers that was intended to be sent to Human Resources was instead sent to an individual at one of Autoliv's vendors with a similar name.

Attribution 1 Publication: NH AG's office Author:
Article Title: Autoliv ASP, Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/autoliv-20180216.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-14	ASI Construction LLC	CO	3/1/2018	Electronic	Business	Yes - Published #	336

On January 31, 2018, an individual posing as John Bowen e-mailed an ASI Construction LLC employee requesting copies of 2017 W-2s for employees of ASI Constructors, Inc. A Form W-2 generally includes information about an employee's name, address, Social Security number, wages or other income and tax withholdings. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's Office / MT AG's office Author:
Article Title: ASI Construction LLC
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/asi-construction-20180301.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-13	Abeles & Hoffman P.C.	PA	2/13/2018	Electronic	Business	Yes - Published #	237

We recently learned that a limited number of email users were victims of a spear-phishing attack resulting in unauthorized access to those users' email boxes between September 26-28, 2017. After an extensive manual email review, which was concluded on January 18, 2018, we can confirm that the impacted email accounts that were accessed contained some of your personal information, including your full name and Social Security number. (Exposure number per IN AG's office)

Attribution 1 Publication: NH AG's office Author:
Article Title: Abeles & Hoffman P.C.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/abeles-20180213.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-12	Kansas Department for Aging and Disability Services	KS	3/3/2018	Electronic	Government/Military	Yes - Published #	11,000

On February 23, 2018, KDADS became aware of a potential breach of personal or protected health information after an employee sent an unauthorized email containing personal or protected health information to a group of current KDADS business associates. The email contained an attachment which included consumer names, addresses, dates of birth, Social Security numbers, gender, in-home services program participation information and Medicaid identification numbers.

Attribution 1 Publication: kdads.ks.gov / databreaches.net Author:
Article Title: KDADS Notifies Consumers About Potential Breach of Protected Health Information
Article URL: <http://www.kdads.ks.gov/required/AllNewsItems/2018/03/01/kdads-notifies-consumers-about-potential-breach-of-prote>

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

Report Date: 7/2/2018

Page 99 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-11	Applebee's Restaurants	NE	3/2/2018	Electronic	Business	Yes - Unknown #	Unknown

It's confirmed that some locations of the Applebee's restaurant chain suffered a point-of-sale (POS) breach involving customers' payment card data. The franchisee believes the incident might have exposed customers' names and payment card details "processed during limited time periods."

Attribution 1 Publication: [tripwire.com / databreaches.net](#) Author:
Article Title: [Applebee's Restaurants](#)
Article URL: <https://www.tripwire.com/state-of-security/latest-security-news/point-of-sale-breach-confirmed-at-some-applebees-loc>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-10	University of Washington	WA	3/5/2018	Electronic	Educational	Yes - Published #	9,000

On Jan. 25, 50 students and 35 faculty and staff members within the Department of Health Services received an email with a spreadsheet that contained personally identifiable information (PII) of more than 9,000 people. This email did not contain dates of birth, Social Security numbers, or financial information that could lead to identity theft, but it did contain name, gender, citizenship status, and ethnicity.

Attribution 1 Publication: [dailyuw.com / databreaches.net](#) Author:
Article Title: [Professor in department of health services unintentionally releases personal student information via email](#)
Article URL: http://www.dailyuw.com/news/article_e0a77a86-201c-11e8-8a8e-d76f00d0261e.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-09	Catawaba County	NC	3/5/2018	Electronic	Government/Military	Yes - Published #	9,182

Catawba County services employees were the subject of a malware attack discovered in October, according to Catawba County Director of Communications Amy McCauley. The security breach was detected in the payroll and human resources section of the system. (Number of Records exposed per NC AG's office)

Attribution 1 Publication: [hickoryrecord.com / databreaches.net /](#) Author:
Article Title: [County employees targets of malware attack](#)
Article URL: http://www.hickoryrecord.com/news/crime/county-employees-targets-of-malware-attack/article_6557562e-209b-11e8-b

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-08	Cindy Nelson & Associates	WA	2/26/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 26, 2018, I learned that an unknown party, during a limited timeframe, may have had the ability to access certain email accounts without authorization. The email accounts included W-2 forms and other tax return information which included your name and Social Security number.

Attribution 1 Publication: [MT AG's office / NY AG's office](#) Author:
Article Title: [Cindy Nelson & Associates](#)
Article URL: <https://dojmt.gov/wp-content/uploads/Nelson-CPA.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-07	Cary E Williams CPA	MS	3/2/2018	Electronic	Business	Yes - Published #	7,690

On January 29, 2018, we discovered that parts of our network were subject to a ransomware attack. This information may have included your: full name, address, Social Security number, and earnings information from that entity. (Exposure number per NC AG's office)

Attribution 1 Publication: [MT AG's office / VT AG's office](#) Author:
Article Title: [Cary E Williams CPA](#)
Article URL: <https://dojmt.gov/wp-content/uploads/Cary-Williams-CPA.pdf>

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

Report Date: 7/2/2018

Page 100 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-05	Cruzstar LLC (MenuDrive)	PA	3/2/2018	Electronic	Business	Yes - Published #	28,740

Last year in 2017, only the Desktop ordering site was attacked and injected with malware intended to capture credit card information while it was being submitted to our site. (Exposure number per NC AG's office)

Attribution 1 Publication: CA AG's office / NY AG's office Author:
Article Title: Cruzstar LLC (MenuDrive)
Article URL: https://oag.ca.gov/system/files/Notification_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-04	MJ Freeway Business Solutions	CO	3/1/2018	Electronic	Business	Yes - Unknown #	Unknown

On or about November 19, 2016, MJ Freeway's systems were accessed without authorization. MJ Freeway determined that the unauthorized individual acquired the following types of information relating to Harborside customers: name and driver's license number.

Attribution 1 Publication: CA AG's office / NY AG's office Author:
Article Title: MJ Freeway Business Solutions
Article URL: https://oag.ca.gov/system/files/MJF%20--%20Notice%20for%20Harborside%20Mailing%20-%20All%20Exhibits_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-03	Rockdale ISD	TX	3/2/2018	Electronic	Educational	Yes - Unknown #	Unknown

An email phishing scheme caused several Rockdale ISD employees' taxes to be falsely filed and compromised confidential tax information for all employees in the district, officials confirmed to KVUE Thursday morning.

Attribution 1 Publication: kvue.com Author:
Article Title: Rockdale ISD employees' tax information compromised in data breach
Article URL: <http://www.kvue.com/article/news/local/rockdale-isd-employees-tax-information-compromised-in-data-breach/269-524>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-02	St. Louis Community College	MO	3/1/2018	Electronic	Educational	Yes - Published #	362

The school says an email attachment containing personally identifiable information for 362 students was sent to a small number of other students. The attachment has names, email, ID numbers and home addresses of the 362 students.

Attribution 1 Publication: kmov.com Author:
Article Title: St. Louis Community College investigating possible
Article URL: <http://www.kmov.com/story/37628377/st-louis-community-college-investigating-possible-student->

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180306-01	Ventiv	IL	3/1/2018	Electronic	Business	Yes - Published #	239

On January 4, 2018, the investigation determined that an unknown individual had accessed certain Ventiv employees' email accounts hosted on Office365 without authorization between October 14, 2017 to December 8, 2017. The emails and attachments that were in the accounts may have included your name and certain information relating to the treatment of your workers' compensation injury. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NY AG's office Author:
Article Title: Ventiv
Article URL: <https://oag.ca.gov/ecrime/databreach/reports/sb24-134144>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-11	University of North Georgia	GA	2/27/2018	Electronic	Educational	Yes - Unknown #	Unknown

On Monday, Feb. 26, the University of North Georgia's Office of University Relations emailed all students regarding improper access of Banner information in January. The information accessed was primarily directory-level data, specifically name, ID number, gender, major, concentration, dorm or commuter status, class, address, phone number, adviser name, email and campus.

Attribution 1 Publication: ungvanguard.org Author:
Article Title: Former UNG employee accessed protected student data in Banner
Article URL: <http://ungvanguard.org/2018/02/in-banner-security-breach-former-employee-accessed-protected-student-data/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-10	Tufts Associated Health Maintenance Organization, Inc.	MA	2/16/2018	Paper Data	Medical/Healthcare	Yes - Published #	70,320

The window of the envelope used for the mailing showed the Tufts Health Plan member ID number, in addition to the member's name and address.

Attribution 1 Publication: [hhs.gov / databreaches.net](http://hhs.gov/databreaches.net) / Tufts Health Author:
Article Title: Tufts Associated Health Maintenance Organization
Article URL: <https://www.databreaches.net/tufts-health-plan-notifies-70320-members-after-vendor-error-exposes-information-in-env>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-09	Association for Supervision and Curriculum Development	VA	2/27/2018	Electronic	Business	Yes - Published #	192

Please be advised that on February 21, 2018, ASCD discovered it experienced an electronic/email communications scam intended to steal data, otherwise known as a "spearphishing attack". The personal information on a W-2 includes your name, address, and social security number. (Exposure number per NC AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Association for Supervision and Curriculum Development
Article URL: <https://dojmt.gov/wp-content/uploads/Association-for-Supervision-and-Curriculum-Development-ASCD.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-08	Active Network	TX	2/23/2018	Electronic	Business	Yes - Published #	207

During this time period, personal information that you provided as part of the checkout process may have been accessed by unauthorized third parties. The information may have included your name, address, email address, credit or debit card number, expiration date, and cardholder verification code (the three- or four-digit value included on the front or back of payment cards and used for verification of certain transactions). (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office Author:
Article Title: Active Network
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/active-20180223.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-07	Pennsylvania Department of Education	PA	2/26/2018	Electronic	Government/Military	Yes - Published #	300,000

A data breach of a state Department of Education database may have potentially compromised personal information including Social Security numbers of Pennsylvania's current and former teachers. The breach, which occurred between 12 noon and 12:30 p.m. on Thursday, was caused by an error made by an employee in the governor's Office of Administration, said Dan Egan, a spokesman for that office.

Attribution 1 Publication: pennlive.com Author:
Article Title: Data breach may have put Pa. teachers' personal information at risk
Article URL: http://www.pennlive.com/politics/index.ssf/2018/02/data_breach_may_have_put_pa_te.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-06	NIS America	CA	2/28/2018	Electronic	Business	Yes - Unknown #	Unknown

On the morning of February 26th, we became aware of a malicious process that had attached itself to our checkout page. The skimming process had access to all information provided by the customer during checkout, including their name, address, credit card number, expiration date and CVV security code, and email address.

Attribution 1 Publication: resetera.com / databreaches.net Author:
Article Title: NIS America
Article URL: <https://www.resetera.com/threads/nisa-online-store-data-breach.26440/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-05	Memorial Hospital at Gulfport	MS	2/28/2018	Electronic	Medical/Healthcare	Yes - Published #	1,512

Memorial Hospital at Gulfport has notified approximately 1,500 patients of an inadvertent disclosure of information, including patient names and internal (Memorial) encounter numbers, that was discovered during a routine internal audit. (Exposure number per HHS)

Attribution 1 Publication: Company website Author:
Article Title: Memorial Hospital at Gulfport
Article URL: <http://www.gulfportmemorial.com/news/memorial-hospital-reports-inadvertent-disclosure-413>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-04	Jemison Internal Medicine of Alabama	AL	2/16/2018	Electronic	Medical/Healthcare	Yes - Published #	6,550

On December 20, 2017, JIM's computer system was infected by a ransomware virus that encrypted our electronic medical records ("EMR") system containing our patients' medical records. In that regard, it is possible that this unauthorized individual could have accessed files in our EMR system, which include patient names, addresses, telephone numbers, Social Security numbers, dates of birth, driver's license numbers, treatment and procedure information, prescription information, and healthcare insurance information.

Attribution 1 Publication: hhs.gov / MD AG's office Author:
Article Title: Jemison Internal Medicine of Alabama
Article URL: <http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-295107.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-03	Country Mutual Insurance Company (Country Financial)	IL	2/23/2018	Electronic	Banking/Credit/Financial	Yes - Published #	1,390

On January 29, 2018, COUNTRY Financial® was notified that the U.S. Postal Service failed to deliver a COUNTRY Financial® package and has been unable to track its current location. This package contained Federal Crop Insurance documents with your personal information including the following: Name, Address, Social Security Number, Policy Number, Account Number (Exposure number per NC AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-02	Aldi	IL	2/28/2018	Electronic	Business	Yes - Unknown #	Unknown

Aldi said Wednesday a recent data breach in which two men reportedly installed bank card skimmers at two Montgomery County stores did not affect shoppers at any of its five Lehigh Valley stores.

Attribution 1 Publication: mccall.com Author:
Article Title: Aldi says some stores hit by data breach
Article URL: <http://www.mcall.com/business/mc-biz-aldi-security-credit-skimmers-20180228-story.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180301-01	Marine Corps Forces Reserve	DC	2/28/2018	Electronic	Government/Military	Yes - Published #	21,426

Roughly 21,426 people were impacted when an unencrypted email with an attachment containing personal confidential information was sent to the wrong email distribution list Monday morning. The compromised attachment included highly sensitive data such as truncated social security numbers, bank electronic funds transfer and bank routing numbers, truncated credit card information, mailing address, residential address and emergency contact information

Attribution 1 Publication: marinecorpstimes.com Author:
Article Title: Major data breach at Marine Forces Reserve impacts thousands
Article URL: <https://www.marinecorpstimes.com/news/your-marine-corps/2018/02/28/major-data-breach-at-marine-forces-reserve-i>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-11	Curtis Lumber Co.	NY	2/26/2018	Electronic	Business	Yes - Published #	579

Early evening on February 23, 2018, we determined that on February 5, 2018, Curtis Lumber Company, Inc. was the subject of a spear phishing incident that resulted in your information being released to an unknown person or persons. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NY AG's office Author:
Article Title: Curtis Lumber Co.
Article URL: <http://ago.vermont.gov/blog/2018/02/26/curtis-lumber-co-sbn-consumers-redacted/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-09	St. Peter's Surgery & Endoscopy Center	NY	2/28/2018	Electronic	Medical/Healthcare	Yes - Published #	134,512

On January 8, 2018, we learned that an unauthorized third party gained access to our servers on that same day. As a patient previously treated at the Center, your information was contained on the servers in question, and would have included your name, date of birth, address, dates of service, diagnosis code, procedure codes and Medicare information (which contains your social security number).

Attribution 1 Publication: VT AG's office / hipaajournal.com / hhs. Author:
Article Title: St. Peter's Surgery & Endoscopy Center
Article URL: <https://www.hipaajournal.com/new-york-surgery-endoscopy-center-discovers-135000-record-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-08	Bed Bath & Beyond	NJ	2/21/2018	Electronic	Business	Yes - Published #	200

We are writing to inform you that during a remodel of Bed Bath & Beyond Store# 68 in Denver, we discovered that a file cabinet containing some personnel documents was inadvertently discarded. As you may know, information in your personnel file and/or on your Form 1-9 documents may include your name, address, social security number, driver's license number, direct deposit information and benefit enrollment information. (Number of Records exposed per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-07	Walmart, Inc.	AR	2/22/2018	Electronic	Medical/Healthcare	Yes - Published #	735

On January 29, 2018, we determined that an internal error affected your pharmacy account profile, which may have caused information about you to be visible to another patient. The personal information potentially viewed could include your name, any contact information in your account (such as postal address, email address, and phone number), your date of birth, insurance information such as your card holder number, and some of your prescription history (such as name of prescription medication filled by Walmart, name of prescriber, and refill dates).

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



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-06	Santa Cruz Biotechnology	CA	2/22/2018	Electronic	Medical/Healthcare	Yes - Published #	2,657

On Monday, December 18, 2017, we discovered that a burglary had occurred in our Santa Cruz office on or around December 17, 2017. It is possible that the following personal information may have been accessed and acquired as a result of this incident: full name, postal address, date of birth, Social Security number, medical and health insurance information, and work-related evaluations. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NY AG' Author:
 Article Title: Santa Cruz Biotechnology
 Article URL: https://oag.ca.gov/system/files/TEMPLATE_Santa_Cruz_Biotechnology_Consumer_Notification_Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-05	California College of the Arts	CA	2/26/2018	Electronic	Educational	Yes - Published #	2,709

On Friday January 19, 2018, a California College of Arts (the "College") laptop used by one of our employees was stolen out of the employee's vehicle. The investigation has determined that the following information related to you may have been on the laptop: name, Social Security number. (Exposure number per IN AG's office)

Attribution 1 Publication: CA AG's office / hhs.gov Author:
 Article Title: California College of the Arts
 Article URL: https://oag.ca.gov/system/files/CCA%20-%20Regulator%20Notice%20-%20CA%20-%20FINAL_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-04	Innovative Artists Talent and Literary Agency, Inc.	CA	2/11/2018	Electronic	Business	Yes - Published #	2,151

At approximately 11:00 p.m. on February 11, 2018, Innovative Artists' office located at 1505 10th St., Santa Monica, CA 90401 was burglarized. The information stored on the stolen computer equipment, if breached, may have included names, Social Security numbers, birth dates, addresses, and in very limited instances, driver's license numbers, medical information and health insurance information. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NY AG's office Author:
 Article Title: Innovative Artists Talent and Literary Agency, Inc.
 Article URL: https://oag.ca.gov/system/files/US%20Notice_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-03	Union Lake Market / ShopRite / Wakefern Group Corp.	NJ	2/28/2018	Electronic	Medical/Healthcare	Yes - Published #	9,956

Nearly 10,000 customers who signed for pharmacy purchases at the ShopRite in Millville have been exposed to a possible data breach after the electronic device used to record those transactions was thrown out in June. Personal information that could have been stored on the device includes name, phone number, date of birth, prescription number, medication name, date and time of pick-up or delivery, signature and zip code.

Attribution 1 Publication: NJ.com / hipaajournal.com / hhs.com Author:
 Article Title: ShopRite pharmacy security breach affects 10K customers
 Article URL: http://www.nj.com/cumberland/index.ssf/2018/02/10000_customers_affected_by_shotrite_pharmacy_secu.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-02	Metro Wire Rope Corporation	NJ	2/27/2018	Electronic	Business	Yes - Published #	108

The investigation determined that the Metro Wire employee received a phishing email containing an attachment with credential stealing capabilities. Through the programmatic and manual review of the employee email account, we determined on January 16, 2018, that the following information related to you may have been contained in the employee's email account at the time it was accessed by the unknown individual(s): <<ClientDef1{first and last name, [credit card information/financial account data/driver's license number]}>> (Exposure number per NC AG's office)

Attribution 1 Publication: VT AG's office / MD AG's office Author:
 Article Title: Metro Wire Rope Corporation
 Article URL: <http://ago.vermont.gov/blog/2018/02/27/metro-wire-rope-sbn-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180228-01	FastHealth Corporation (multiple entities)	AL	2/28/2018	Electronic	Medical/Healthcare	Yes - Published #	657,529

On November 2, 2017, FastHealth received a report from law enforcement indicating that an unauthorized third party may have accessed or acquired certain information from FastHealth databases. (Type of exposed information and exposure number per NC AG's office)

Attribution 1 Publication: VT AG's office / CA AG's office / OR AG' Author:
Article Title: FastHealth Corporation
Article URL: https://oag.ca.gov/system/files/California%20Notice%20Samples_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180226-07	American Neighborhood Mortgage Acceptance Company dba AnnieMac	NJ	2/16/2018	Electronic	Banking/Credit/Financial	Yes - Published #	109

Between September 15, 2017 and September 28, 2017, unauthorized parties accessed certain AnnieMacHome Mortgage employee email accounts through an email phishing scheme. The information accessed included: Social Security number; Tax returns; First and last name; Address; and Phone number. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office Author:
Article Title: American Neighborhood Mortgage Acceptance Company dba AnnieMac Home Mortgage
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/anniemac-20180216.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180226-06	Chase.com (JP Morgan Chase)	NY	2/22/2018	Electronic	Banking/Credit/Financial	Yes - Published #	7,977

Multiple Chase.com customers have reported logging in to their bank accounts, only to be presented with another customer's bank account details. (Exposure number per NY AG's office)

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Chase 'Glitch' Exposed Customer Accounts
Article URL: <https://krebsonsecurity.com/2018/02/chase-glitch-exposed-customer-accounts/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180226-05	City of Houston Medical Plan	TX	2/23/2018	Electronic	Government/Military	Yes - Published #	34,637

City officials say the laptop was stolen from the employee's car on Feb. 2. They say the password-protected computer may have contained city employees' records, including names, addresses, dates of birth, Social Security numbers and other medical information.

Attribution 1 Publication: khou.com / hhs.gov Author:
Article Title: Sensitive info may be compromised after City of Houston employee's laptop stolen
Article URL: <http://www.khou.com/article/news/local/sensitive-info-may-be-compromised-after-city-of-houston-employees-laptop-stolen>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180226-04	Wallace Community College Selma	AL	2/24/2018	Electronic	Educational	Yes - Unknown #	Unknown

Personal and financial information of current and former employees of Wallace Community College Selma has been accidentally leaked through a phishing scam, according to an attorney representing the school. W-2 forms, which are used to file for income tax returns, contain pertinent information, such as social security number, name, address, employer information, wage, etc.

Attribution 1 Publication: selmatimesjournal.com Author:
Article Title: Cyber criminals target Wallace employees
Article URL: <http://www.selmatimesjournal.com/2018/02/24/cyber-criminals-target-wallace-employees/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180226-03	Mueller and Company LLP	IL	2/23/2018	Electronic	Business	Yes - Published #	2,921

On February 12, 2018, the forensic investigator informed us that in November, 2017, an unauthorized third party had accessed a computer system in MPS's Orland Park location. This computer contained files related to tax returns prepared at the Orland Park office and may have contained your name, address, Social Security number, wage information and bank account information if you provided it to us. (Exposure number per NC AG's office)

Attribution 1 Publication: VT AG's office / NY AG's office / NC AG' Author:
Article Title: Mueller and Company LLP
Article URL: <http://ago.vermont.gov/blog/2018/02/23/mueller-co-cpa-sbn-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180226-02	North 40 Outfitters	MT	2/23/2018	Electronic	Business	Yes - Published #	14,734

On or about January 10, 2018, North 40 was alerted by its card processor that certain credit and debit cards used on its e-commerce site may have been subject to unauthorized use. The information that could have been subject to unauthorized access includes customer names, credit or debit card numbers, card expiration date, and card security number or CVV. Certain customers' North 40 user account names and passwords may also have been affected. (Exposure number per NC AG's office)

Attribution 1 Publication: VT AG's office / CA AG's office / OR AG' Author:
Article Title: North 40 Outfittersw
Article URL: https://oag.ca.gov/system/files/North%2040-%20California%20Form%20Exhibit%201_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180226-01	University of Wisconsin - Superior	WI	2/22/2018	Electronic	Educational	Yes - Published #	3,734

In the process of preparing the mailing data, an ID number was sent to our travel vendor and appeared above your name and address on the brochure. On February 5, 2018, we were made aware that the ID number for our alumni who graduated during a certain time period may have been the same as the student ID number (social security number) used while in attendance at UW-Superior. The personal information that may have been viewable on the brochure included first and last names, home addresses and social security numbers. (Exposure number per NC AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180221-02	University of Virginia Health System	VA	2/21/2018	Electronic	Medical/Healthcare	Yes - Published #	1,882

On December 23, 2017, University of Virginia Health System learned that this third party may have been able to view patient information on these devices from May 3, 2015, to December 27, 2016. The investigations could not rule out that the third party may have been able to view some patient information, which may have included patients' names, diagnoses, treatment information, addresses and dates of birth.

Attribution 1 Publication: NBC29.com / databreaches.net / hipaajo Author:
Article Title: UVA Health System Notifies 1,882 Patients About Potential Privacy Issue
Article URL: <http://www.nbc29.com/story/37555891/uva-health-system-notifies-1882-patients-about-potential-privacy-issue>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180221-01	Los Angeles Philharmonic	CA	2/20/2018	Electronic	Business	Yes - Published #	2,442

The Los Angeles Philharmonic was the victim of a targeted email spoofing scheme on February 14, 2018. A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. (Exposure number per IN AG's office)

Attribution 1 Publication: VT AG's office / CA AG's office Author:
Article Title: Los Angeles Philharmonic
Article URL: <https://oag.ca.gov/system/files/LA%20Philharmonic%20-%20Notice%20of%20Data%20Event%20-%20CA%20-%20Ex%2>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-14	Chapman Mortgage Services (Motto Mortgage of Billings)	MT	2/15/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We promptly began investigating this matter and believe that an unauthorized unknown individual or individuals gained access to our email database through a phishing attack. Our investigation indicates that personal information contained in uniform residential mortgage applications, closing documents, and related communications, including names, addresses, social security numbers, drivers license numbers, and account information, was accessible to the unknown actors.

Attribution 1 Publication: MT AG's office Author:
 Article Title: Chapman Mortgage Services (Motto Mortgage of Billings)
 Article URL: <https://dojmt.gov/wp-content/uploads/Chapman-Mortgage-Services.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-13	Bialy/Thomas & Associates	CA	2/16/2018	Electronic	Business	Yes - Published #	781

From what we can tell, an unauthorized person or persons successfully perpetrated a phishing attack and used the compromised account credentials to send a number of suspicious emails on November 16, 2017, at which time we became aware of the compromise and took immediate steps to secure the account. While the investigation continues, our current understanding is that the affected personal information may include your Social Security number, government-issued ID information (such as a driver's license number, passport number, Tax ID number, or Employer Identification Number); and/or online account credentials. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NY AG's office Author:
 Article Title: Bialy/Thomas & Associates
 Article URL: <https://dojmt.gov/wp-content/uploads/Bialy-Thomas-and-Associates.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-12	White and Bright Dental	CA	2/19/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Fresno, CA-based White and Bright Family Dental has discovered one of its servers containing patients' protected health information has been accessed by hackers. An analysis of the server revealed the following types of information were potentially accessed: Names, addresses, telephone numbers, birth dates,

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
 Article Title: Patients Notified of White and Bright Family Dental Server Hack
 Article URL: <https://www.hipaajournal.com/patients-notified-white-bright-family-dental-server-hack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-11	Ascensus	PA	2/21/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 31, 2018, Ascensus inadvertently sent a payroll report to another Ascensus retirement plan client. Upon discovering this, Ascensus immediately informed the recipient that she had received confidential data in error. The report contains your name, address, birth date, date of hire and Social Security number.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Ascensus (Red Hawk Casino)
 Article URL: https://oag.ca.gov/system/files/221725%20Red%20Hawk%20Casino%20-%20Individual%20Letter_1.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-10	Weaver & Tidwell, LLP (CCH Client Access)	TX	2/9/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 10, 2018, CCH informed Weaver that an unauthorized person was able to log into a Weaver partner's CCH account after successfully guessing the answer to a security question. These documents may have included clients' name, Social Security number, and financial account information.

Attribution 1 Publication: NH AG's office Author:
 Article Title: Weaver & Tidwell, LLP (CCH Client Access)
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/weaver-20180209.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-09	Department of Mental Health	MO	2/16/2018	Electronic	Government/Military	Yes - Published #	1,000

The Missouri Department of Mental Health is notifying 1,000 people that some personal information might have been mailed to an incorrect address.

Attribution 1 Publication: [fox2now.com / databreaches.net](#) Author:
 Article Title: Missouri Department of Mental Health
 Article URL: <http://fox2now.com/2018/02/16/missouri-mental-health-department-admits-mailing-error/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-08	HomeTown Bank, N.A.	TX	2/18/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On January 19, 2018, HomeTown Bank, N.A. ("HomeTown") discovered that a skimming/shimming device had been placed on an ATM at the bank's branch located at 4424 Seawall Blvd, Galveston, TX 77551. The device may have acquired the following of the affected individuals' personal information that was stored on the cards used in connection with such transactions during the relevant time period: individuals' names, card numbers, card expiration dates and personal identification numbers (PINs).

Attribution 1 Publication: [galvnews.com / databreaches.net](#) Author:
 Article Title: HomeTown Bank, N.A.
 Article URL: http://www.galvnews.com/classifieds/service/legal/pdfdisplayed_8eb14c78-1371-11e8-8002-677a74384e0a.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-07	Medical Science & Computing, LLC	MD	2/13/2018	Electronic	Medical/Healthcare	Yes - Published #	137

On or about January 29, 2018, MSC mistakenly emailed a file containing W2 forms for 137 MSC employees. The information subject to unauthorized disclosure includes your name and Social Security number. (Exposure number per NC AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: Medical Science & Computing, LLC
 Article URL: <https://dojmt.gov/wp-content/uploads/Medical-Science-Computing-LLC.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-06	Thomas Edison State University	NJ	2/13/2018	Electronic	Educational	Yes - Published #	557

We determined through our investigation that an intruder gained access to the email account of one Thomas Edison employee. The information related to you that was contained in the impacted email account during the period in question included your name and Social Security number. (Exposure number per NC AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-05	PACCAR Financial	TX	2/14/2018	Electronic	Banking/Credit/Financial	Yes - Published #	251

On January 22, we learned that a company laptop and USB thumb drive were stolen from a locked vehicle. The stolen devices may have contained your name and contact information; a credit application containing your social security number, credit information, and date of birth; and a photocopy of your driver's license, if it was provided to us. (Number of Records exposed per IN AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-04	Flexible Benefit Service Corporation (FLEX)	IL	2/14/2018	Electronic	Medical/Healthcare	Yes - Published #	19,438

We have determined the Flex employee was the victim of a phishing attack that resulted in their email account credentials being used by unknown individual(s) to gain unauthorized access to the employee's email account. We determined on January 30, 2018, that the following information related to you may have been contained in the employee's email account at the time it was accessed by the unknown individual(s): <IMPACTED DATA ELEMENT(S)> and name. (Exposure number per NC AG's office)

Attribution 1 Publication: MT AG's office Author:
Article Title: Flexible Benefit Service Corporation (FLEX)
Article URL: <https://dojmt.gov/wp-content/uploads/Flexible-Benefit-Service-Corporation.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-03	American Stock Transfer & Trust Company, LLC (Colony Northstar Credit Real Estate)	NY	2/16/2018	Electronic	Business	Yes - Unknown #	Unknown

AST serves as the exchange agent for a transaction involving Colony NorthStar Credit Real Estate, Inc. (the "Company"). On February 1, 2018, an AST employee sent a file containing information about shareholders of the Company (the "Shareholder Information") to 34 financial advisors who represent those shareholders. The Shareholder Information included name, address, social security number, financial account information relating to ownership of the Company's shares, as well as information relating to the designated financial advisor

Attribution 1 Publication: CA AG's office Author:
Article Title: American Stock Transfer & Trust Company, LLC
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_21.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-02	Department of Fish and Wildlife	CA	2/14/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

A former employee downloaded personally identifiable information to an unencrypted personal device and took the data outside of CDFW's secure network. The data contained first name, last name, and social security numbers and, for a limited number of individuals the data included home addresses.

Attribution 1 Publication: CA AG's office Author:
Article Title: Callifornia Department of Fish and Wildlife
Article URL: https://oag.ca.gov/system/files/CDFW%20Breach%20Notification-Final_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180220-01	Driscoll's, Inc.	CA	2/13/2018	Electronic	Business	Yes - Published #	1,530

On or about July 28, 2017, Driscoll's determined that some employees' payroll log-in credentials were compromised when the employees responded to a phishing email. The information related to you that was contained within one of the email accounts included your name and one or more of Social Security number, driver's license number, Passport number, credit/debit card number, bank account information, medical information and health insurance information. (Number of Records exposed per NC AG's office)

Attribution 1 Publication: CA AG's office Author:
Article Title: Driscoll's, Inc.
Article URL: <https://oag.ca.gov/system/files/Driscoll%27s%20-%20Notice%20of%20Data%20Event%20-%20CA%20-%20Exhibit%201>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180216-07	Etsy	NY	2/15/2018	Electronic	Business	Yes - Published #	1,566

Etsy confirmed a privacy breach impacted about 1,500 sellers. The incident was caused by human error and was not related to any hacking or website vulnerability. The form contains the tax identification number (TIN) of the payer (in this case Etsy) and the payee (in this case, sellers). In some cases, sellers (particularly low-volume sellers) use their social security number as their TIN. We have a follow-up question in to Etsy about whether it used the full social security number on 2016 forms, or just the last 4 digits. (Number of Records exposed per NY AG's office)

Attribution 1 Publication: ecommercebytes.com / NY AG's office Author:
Article Title: Etsy Discloses Tax-Related Privacy Breach
Article URL: <https://www.ecommercebytes.com/2018/02/15/etsy-discloses-tax-related-privacy-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180216-06	Western Union	CO	2/14/2018	Electronic	Business	Yes - Unknown #	Unknown

"We have discovered that some of your information may have been accessed without authorization as a result of a computer intrusion against an external vendor system formerly used by Western Union for secure data storage," the letter said. • Customer contact details • Bank names • Western Union internal customer ID numbers • Transaction amounts and times • Identification numbers

Attribution 1 Publication: wccfttech.com Author:
Article Title: Western Union Customer Data Stolen – Company Blames an Unnamed Storage Firm
Article URL: <https://wccfttech.com/western-union-customer-data-stolen/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180216-05	Engle Martin & Associates, Inc.	GA	2/14/2018	Electronic	Business	Yes - Published #	2,508

The forensic investigator notified us that an unauthorized user had obtained access to the email addresses of a limited number of Engle Martin employees. On January 3, 2018, our forensic vendor alerted us that these email accounts contained information that may have included your name, address, Social Security number, health insurance information, or other demographic information. (Number of Records exposed per NC AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Engle Martin & Associates, Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/engle-martin-associates-20180214.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180216-04	LendKey Technologies, Inc.	NY	2/15/2018	Electronic	Banking/Credit/Financial	Yes - Published #	6,403

On or about December 21, 2017, LendKey learned that certain consumer loan application data sent by email, and contained on one of our computer servers, may have been accessible to the internet since June 27, 2016. (Number of Records exposed per IN AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180216-03	Peoples United Bank	VT	2/15/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

A copy of your home equity application and disclosures containing your name, social security number, date of birth, address, and other personal information was inadvertently emailed to a third party.

Attribution 1 Publication: VT AG's office Author:
Article Title: Peoples United Bank
Article URL: <http://ago.vermont.gov/blog/2017/02/16/peoples-united-bank-sbn-to-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180216-02	FedEx / Bongo	TN	2/15/2018	Electronic	Business	Yes - Published #	119,000

Thousands of FedEx customers were exposed after the company left scanned passports, drivers licenses, and other documentation on a publicly accessible Amazon S3 server.

Attribution 1 Publication: gizmodo.com Author:
Article Title: 119,000 Passports and Photo IDs of FedEx Customers Found on Unsecured Amazon Server
Article URL: <https://gizmodo.com/119-000-passports-and-photo-ids-of-fedex-customers-foun-1823035669>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180216-01	Staybridge Suites Lexington	KY	2/15/2018	Electronic	Business	Yes - Published #	244

A hotel in Lexington is letting customers know about a data breach which may have given unauthorized people access to names and credit card numbers. The Staybridge Suites Lexington says it received a notice that certain electronic devices were infected with malware. (Number of records exposed per NC AG's notification)

Attribution 1	Publication: wkyt.com	Author:
	Article Title: Lexington hotel says customer credit card numbers exposed in data breach	
	Article URL: http://www.wkyt.com/content/news/Lexington-hotel-says-customer-credit-card-numbers-exposed-in-data-breach-4741	

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180214-04	OneMain Financial	IN	2/9/2018	Electronic	Banking/Credit/Financial	Yes - Published #	1,253

OneMain recently determined that an unauthorized individual(s) apparently compromised the personal or work e-mail accounts of OneMain customers, and used the e-mail accounts between September 1, 2017 and January 16, 2018 to access certain customer's OneMain online accounts. The personal information involved in this incident may have included first and last name, phone number, OneMain loan account number, OneMain Rewards account, and type of insurance purchased for a OneMain loan account, if applicable. (Number of Records exposed per NC AG's office)

Attribution 1	Publication: NH AG's office	Author:
	Article Title: OneMain Financial	
	Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/onemain-financial-20180209.pdf	

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180214-03	Citizens Financial Group, Inc. (multiple locations)	RI	2/2/2018	Electronic	Banking/Credit/Financial	Yes - Published #	262

The skimming events took place on various dates on January 18-23, 2018 and were discovered by Citizens on January 23, 2018. Customer name, debit card number, and PIN were compromised as a result of this incident. (Exposure number per NY AG's office)

Attribution 1	Publication: NH AG's office / NY AG's office	Author:
	Article Title: Citizens Financial Group, Inc. (multiple locations)	
	Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-20180202.pdf	

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180214-02	Midland School District	AR	2/12/2018	Electronic	Educational	Yes - Published #	100

For whatever reason, the school evidently became a collection point for student records from throughout the Midland district. Ziebell said he has birth certificates, Social Security numbers and "everything else" for about 100 students.

Attribution 1	Publication: qctimes.com / databreaches.net	Author:
	Article Title: Ickes: This time, students' records left behind	
	Article URL: http://qctimes.com/news/local/barb-ickes/ickes-this-time-students-records-left-behind/article_5692f141-8687-519d-841	

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180214-01	Massachusetts Department of Revenue / MassTaxConnect	MA	2/13/2018	Electronic	Government/Military	Yes - Published #	39,000

A data mix-up on a state tax portal inadvertently made private data from about 16,500 business taxpayers viewable to other companies, potentially even competitors. The breach lasted from Aug. 7, 2017, through Jan. 23, 2018, and allowed some companies to view other business's names, federal employer identification numbers, tax payments, and other data, according to the Massachusetts Department of Revenue.

Attribution 1	Publication: bostonglobe.com	Author:
	Article Title: Yikes! Data breach at Mass. tax agency allowed companies to peek in on competitors' data	
	Article URL: http://www.bostonglobe.com/business/2018/02/13/yikes-data-breach-mass-tax-agency-allowed-companies-peek-comp	

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180213-07	Inspire Home Loans	CA	2/9/2018	Electronic	Banking/Credit/Financial	Yes - Published #	2,414

On January 15, 2018, the forensic firm determined that an unauthorized actor had accessed emails in employees' accounts. Our investigation has determined that the affected email accounts contained a message with some of your personal information, including your name, address, and Social Security number. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Inspire Home Loans
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/inspire-home-loans-20180209.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180213-06	QuadMed (Whirlpool)	WI	1/29/2018	Electronic	Medical/Healthcare	Yes - Published #	4,549

On December 26, 2017, QuadMed became aware of a potential technical issue that enabled Hillenbrand employees to access more information than they should have been able to access. Whether that unintended access existed since November 2013 was not clear, but that information included employees' name, date(s) of services or treatment at the onsite clinic, and medical information, such as test or evaluation results, diagnoses, and information related to medical history, examinations, physicals, screenings, vaccinations, travel medicine, and/or workers' compensation information.

Attribution 1 Publication: hhs.gov / databreaches.net Author:
Article Title: QuadMed (Whirlpool)
Article URL: <https://www.databreaches.net/quadmed-health-records-system-issue-affected-onsite-clinics-of-three-clients/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180213-05	Idaho Transportation Department	ID	2/12/2018	Electronic	Government/Military	Yes - Published #	

A hack of two email accounts at the Idaho Transportation Department (ITD) potentially exposed the personal information of commercial truckers whose rigs are registered in Idaho, including Social Security and credit card numbers. One email account that was exposed contained an estimated 318 driver's license numbers, 400 Social Security numbers or employee ID numbers, 999 credit card numbers, and 11 bank account numbers.

Attribution 1 Publication: eastidahonews.com / databreaches.net Author:
Article Title: ITD email hack may have exposed truckers' private information
Article URL: <https://www.eastidahonews.com/2018/02/itd-email-hack-may-have-exposed-truckers-personal-information/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180213-04	Livingston County Schools	KY	2/13/2018	Electronic	Educational	Yes - Unknown #	Unknown

Superintendent Victor Zimmerman apologized Monday night for unknowingly posting payroll information with social security numbers on the Livingston County school district's website.

Attribution 1 Publication: wpsdlocal6.com / databreaches.net Author:
Article Title: Livingston County Schools teachers, staff fear identity theft
Article URL: <https://www.databreaches.net/?s=livingston&searchsubmit=>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180213-03	RoxSan Pharmacy	CA	2/13/2018	Electronic	Medical/Healthcare	Yes - Published #	1,049

However, since the data file was transmitted for non-health-related reasons, the transmission is considered a breach. The unsecured information includes records dated between April 2015 and August 2015, and includes prescription information, patient identification numbers, drug information, physician names, and insurance information.

Attribution 1 Publication: RoxSan Pharmacy press release Author:
Article Title: RoxSan Pharmacy Notifies Patients of Breach That Occurred in 2015
Article URL: <https://www.prnewswire.com/news-releases/roxsan-pharmacy-notifies-patients-of-potential-breach-of-unsecured-pers>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180213-02	Blink Health	NY	2/5/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On January 18, 2018, we discovered a systems error that caused the username and password of a very small number of our users to be inadvertently shared with a Blink Health vendor that assists us in analyzing our website data to improve our customer experience.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180213-01	Mississippi State University	MS	2/12/2018	Electronic	Educational	Yes - Unknown #	Unknown

"It's a serious breach, like any breach of the system is serious if it involves university records. This is not a catastrophic breach," Salter said. "Social Security numbers are not an issue at this point." Salter said a "substantial amount of information" was seized during the search and that it could take up to two weeks to analyze the evidence. (The subject of the search warrant was a former MSU student who was last enrolled in December.)

Attribution 1 Publication: clarionledger.com Author:
 Article Title: Mississippi State University
 Article URL: <https://www.clarionledger.com/story/news/local/2018/02/12/msu-data-breach-not-catastrophic/330348002/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180212-10	Wintrust Mortgage	IL	2/2/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

One Wintrust Mortgage employee was recently the victim of an email phishing attack, which appears to have taken place in early December 2017. However, information that may have been available through the impacted employee's credentials includes names, contact information, social security numbers, driver's licenses or federal identification numbers, dates of birth, financial account numbers and other information connected with Wintrust Mortgage's loan services.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
 Article Title: Wintrust Mortgage
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/wintrust-mortgage-20180202.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180212-09	Make-Up Designory	CA	2/5/2018	Electronic	Business	Yes - Published #	670

We are writing on behalf of our client Make-up Designory to report a data breach that occurred as a result of a mailing error made by our client's service provider when it mailed 1098-T Tuition Statements to its students and graduates. Each January Make-up Designory is required to send a tax document (1098-T Tuition Statement) to its students and graduates, which includes the following information: first and last name, mailing address, social security number, total amount billed for qualified tuition and related expenses and any scholarships or grant totals for the applicable tax year. (Number of Records exposed per IN AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: Make-Up Designory
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/make-up-designory-20180205.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180212-08	Lonza	GA	1/24/2018	Electronic	Business	Yes - Unknown #	Unknown

In the fall of 2017 Lonza employees were exposed to several phishing attempts, some of which resulted in hackers accessing a small number of employees' credentials. As a result, the hackers were able to view an account holder's personal information and reroute direct deposit paychecks into a bank account that they could access.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
 Article Title: Lonza
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/lonza-20180124.pdf>

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

Report Date: 7/2/2018

Page 114 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180212-07	Coca-Cola Company	DE	1/19/2018	Electronic	Business	Yes - Published #	2,181

From approximately July to November 2017, certain employees of Coca-Cola received phishing emails in which they were asked to provide their network log-in credentials. In late September, we identified an instance of unauthorized access into a Coca-Cola employee's email account that resulted from this phishing incident. (Number of Records exposed per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Coca-Cola Company
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/coca-cola-20180119.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180212-06	Appen Butler Hill, Inc.	WA	1/5/2018	Electronic	Business	Yes - Published #	1,584

On October 16, 2017, Appen discovered that one of its employees had been the victim of a phishing attack. Depending on the circumstances relating to each individual, the following personal information may have been accessed and acquired: full name, postal address, email address, date of birth, Social Security number, financial account information, health and disability insurance information, and copies of documents submitted with an I-9 form to establish identity and employment authorization. (Number of Records exposed per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Appen Butler Hill, Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/appen-butler-20180105.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180212-05	City of Thomasville	NC	2/5/2018	Electronic	Government/Military	Yes - Published #	269

City manager Kelly Craver told FOX8 the city accidentally released 269 employees' Social Security numbers to someone who put in a public record request for employee salaries. (Exposure number per NC AG's office)

Attribution 1 Publication: myfox8.com / databreaches.net Author:
Article Title: City of Thomasville admits to releasing employees' Social Security numbers
Article URL: <http://myfox8.com/2018/02/06/city-of-thomasville-admits-to-releasing-employees-social-security-numbers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180212-04	Aperio Group	CA	2/12/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 30, Aperio informed advisors of a data breach that occurred when two employees' email accounts were compromised by successful phishing attacks that resulted in auto-forwarding email from those accounts to two external accounts. The compromised data included account names, account numbers, email addresses, and account balances.

Attribution 1 Publication: databreaches.net Author:
Article Title: Aperio Group client account data breached by successful phishing attack
Article URL: <https://www.databreaches.net/aperio-group-client-account-data-breached-by-successful-phishing-attack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180212-02	Connecticut Airport Authority	CT	2/12/2018	Electronic	Business	Yes - Published #	144

On or about November 14, 2017, CAA learned of phishing emails being sent from certain CAA employees' email accounts. We determined on December 29, 2017, that the following information relating to you was contained in one of the impacted email accounts at the time of this incident. (Driver's license and exposure number per NC AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Connecticut Airport Authority
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/connecticut-airport-authority-20180209.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180212-01	Sutter Health	CA	2/6/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On December 5, 2017 Sutter Health learned that Salem and Green, a vendor providing legal services to Sutter Health, was impacted by a phishing attack. The information potentially accessed included your name, and <date of birth>, <social security number>, <California driver's license number>, <state identification number>, and <other professional identification numbers>.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Sutter Health
Article URL: https://oag.ca.gov/system/files/Sample%20Notification-PDF_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180209-04	Eastern Salt Company, Inc.	MA	2/2/2018	Electronic	Business	Yes - Unknown #	Unknown

On January 29, 2018, Eastern Salt discovered that a file containing personal information of its employees was moved within Eastern's system by an unauthorized person, and may have been viewed. The file contained the names, dates of birth and Social Security numbers of the employees of Eastern Salt and its subsidiary companies.

Attribution 1 Publication: NH AG's office Author:
Article Title: Eastern Salt Company, Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/easatern-salt-20180202.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180209-02	Sacramento Bee	CA	2/8/2018	Electronic	Business	Yes - Unknown #	Unknown

Last month, a local California newspaper left more than 19 million voter records exposed online.

Attribution 1 Publication: gizmodo.com Author:
Article Title: Sacramento Bee Leaks 19.5 Million California Voter Records, Promptly Compromised by Hackers
Article URL: <https://gizmodo.com/sacramento-bee-leaked-19-5-million-california-voter-rec-1822835127>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180209-01	Corporate Employment Resources, Inc.	MI	2/9/2018	Electronic	Business	Yes - Published #	4,086

On January 26, 2018, a Company employee sent an e-mail (the "January 26 e-mail") to several current and former Company employees who were authorized to receive the e-mail but inadvertently attached a document not intended for the recipients. The personal information included first and last names and Social Security numbers. (Number of Records exposed per NC AG's office)

Attribution 1 Publication: VT AG's office / MT AG's office / NH AG' Author:
Article Title: Corporate Employment Resources, Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/corporate-employment-20180208.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180208-04	DiFilippo Corporate Finance Group	MA	2/2/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On January 12, 2018, the forensic investigation determined that an unauthorized user gained access to the email account through a phishing attack and may have been able to open and download emails between December 5 and December 14, 2017. DCFG conducted a detailed review of the impacted account and detennined that a small number of clients ' name and Social Security number were contained in an email attachment.

Attribution 1 Publication: NH AG's office Author:
Article Title: DiFilippo Corporate Finance Group
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/difilippo-20180202.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180208-02	Waldo County	ME	2/8/2018	Electronic	Government/Military	Yes - Published #	100

Between 8:30 and 9 a.m on Feb. 5, someone impersonating a county official requested confidential employee information including W-2 forms compromising employee payroll information, social security numbers and filing addresses, according to the Press Herald.

Attribution 1

Publication: scmagazine.com

Author:

Article Title: Waldo County, Maine, phishing attack results in data breach

Article URL: <https://www.scmagazine.com/waldo-county-maine-employee-data-breached-after-phishing-attack/article/743142/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180208-01	Decatur County General Hospital	TN	1/26/2018	Electronic	Medical/Healthcare	Yes - Published #	24,000

Decatur County General Hospital in Tennessee has discovered malware has been installed on a server housing its electronic medical record system. The attacker potentially gained access to the medical records of up to 24,000 patients.

Attribution 1

Publication: hipaajournal.com / hhs.gov

Author:

Article Title: 24,000 Decatur County General Hospital Patients Notified About Malware-Related Data Breach

Article URL: <https://www.hipaajournal.com/24000-decatur-county-general-hospital-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180207-05	Zachary E. Adkins, DDS	NM	1/25/2018	Electronic	Medical/Healthcare	Yes - Published #	3,677

On November 30, 2017, a laptop bag containing an external hard drive from Dr. Adkins' office was stolen. The files in the Dentrix backup contained patient names, addresses, phone numbers, dates of birth, Social Security numbers, treatment information, and insurance information.

Attribution 1

Publication: hhs.gov / zacharyadkinsdental.com

Author:

Article Title: Zachary E. Adkins, DDS

Article URL: <http://zacharyadkinsdental.com/press-release/5424413>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180207-04	Kinetics Systems, Inc.	CA	2/7/2018	Electronic	Business	Yes - Published #	875

On February 1, 2018, Kinetics Systems, Inc. ("Kinetics") received notice than an inadvertent data exposure occurred on January 25, 2018 (the "Incident"). Kinetics experienced a "phishing" attack-via fraudulent email a scammer posed as an Officer of Kinetics, and obtained personal information of current and past employees who worked at Kinetics during 2017. Kinetics believes the personal information breached included W-2 information, including name, Social Security number, employee number, and wage information. (Exposure number per NY AG's office)

Attribution 1

Publication: NH AG's office

Author:

Article Title: Kinetics Systems, Inc.

Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/kinetics-systems-20180207.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180207-02	Boeing Company	IL	2/7/2018	Electronic	Business	Yes - Unknown #	Unknown

Boeing recently discovered that when a standard company report regarding people with security clearances transferring jobs or locations was generated, social security number was accidentally included. This document was sent out to a large distribution list of government security personnel. The spreadsheet contained your first and last name, information about your security clearance and your social security number.

Attribution 1

Publication: MT AG's office

Author:

Article Title: Boeing Company

Article URL: <https://dojmt.gov/wp-content/uploads/Boeing-2.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180207-01	Ameriprise Financial (2/6/18)	MN	2/6/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We have reason to believe that during these calls, Fred Miller had identified himself as your current Ameriprise Financial Advisor Larry Schultz. In a review of the phone calls, it has been determined that Fred Miller has information pertaining to your accounts with Ameriprise. In particular, the information includes, your name, address, and account numbers.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180206-07	PAR Electrical Contractors, Inc.	CA	2/5/2018	Electronic	Business	Yes - Published #	25,500

On or about December 22, 2017, a thief stole a container holding daily backup tapes that, as part of PAR's regular practices, had been taken off-site. (Number of Records exposed per IN AG's office)

Attribution 1 Publication: VT AG's office / CA AG's office / NH AG' Author:
Article Title: PAR Electrical Contractors, Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/par-electrical-20180205.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180206-06	Wag Labs	CA	1/12/2018	Electronic	Business	Yes - Published #	25,500

The information in question was contained in a set of pages on the Wag Labs site described as "obscure", pages that hadn't been given any level of password protection. (Exposure number per NY AG's office)

Attribution 1 Publication: paymentweek.com / NY AG's office Author:
Article Title: Bad Dog! Wag Labs Socked With Data Breach
Article URL: <https://paymentweek.com/2018-1-12-bad-dog-wag-labs-socked-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180206-05	1st Mariner Bank	MD	2/5/2018	Electronic	Banking/Credit/Financial	Yes - Published #	1,500

1st Mariner became aware of suspicious phishing email messages received by our employees and launched an investigation with the assistance of a leading outside computer forensics expert. Our investigation determined the following types of your personal information were stored within an impacted email account and may have been viewed or downloaded by an unauthorized actor: exposed element 1, exposed element 2, exposed element 3, exposed element 4, exposed element 5, exposed element 6 and name. (Number of Records exposed per IN AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180206-04	Bunge Milling	MO	2/6/2018	Electronic	Business	Yes - Unknown #	Unknown

Last summer, an employee at the Crete operation sent personal information via email to a person she thought was a Bunge executive, Seidel said.

Attribution 1 Publication: journalstar.com Author:
Article Title: Crete workers victims of email scam
Article URL: http://journalstar.com/business/local/crete-workers-victims-of-data-breach/article_2f650ff1-5bf7-551e-b469-b2669bd62

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

Report Date: 7/2/2018

Page 118 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180206-03	City of Detroit	MI	2/5/2018	Electronic	Government/Military	Yes - Published #	544

City of Detroit MI Healthcare Provider 544 02/05/2018 Loss Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
 Article Title: City of Detroit
 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
ITRC20180206-02	City of Pittsburg	KS	2/5/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

Personal data belonging to employees of the city of Pittsburg was released to scammers in a phishing attack on Jan. 30, according to a statement from the city. Before the messages were recognized as fakes, the city released information belonging to current and former city employees who received a W-2 for the 2017.

Attribution 1 Publication: joplinglobe.com Author:
 Article Title: City of Pittsburg targeted in phishing attack
 Article URL: http://www.joplinglobe.com/news/crime_and_courts/city-of-pittsburg-targeted-in-phishing-attack/article_b82eed90-7cf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180206-01	Partners HealthCare System	MA	2/5/2018	Electronic	Medical/Healthcare	Yes - Published #	2,600

The breach was a malware incident that was discovered on May 8, 2017 when the healthcare system's intrusion monitoring system detected suspicious activity. The types of information that could potentially have been accessed included names, service dates, and limited clinical information such as diagnoses, procedure types, and medications. Some patients also had their Social Security and financial information exposed.

Attribution 1 Publication: hipaajournal.com / NH AG's office / hhs. Author:
 Article Title: Partners HealthCare System
 Article URL: <https://www.hipaajournal.com/partners-healthcare-notifies-2600-patients-may-2017-breach-phi/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-11	City of Batavia	IL	2/2/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

Someone sent an email, designed to look like it was from Newman, to an employee. It asked the worker to supply W-2 information. The city has also notified the IRS and the Illinois Department of Revenue that someone may try to file fraudulent tax returns using the information, which included the employees' names, addresses and wages.

Attribution 1 Publication: dailyherald.com Author:
 Article Title: Some Batavia city employees' personal data stolen in spoofing attack
 Article URL: <http://www.dailyherald.com/news/20180202/some-batavia-city-employees-personal-data-stolen-in-spoofing-attack>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-09	Octoly	NY	2/5/2018	Electronic	Business	Yes - Published #	12,000

More than 12,000 prominent social media influencers from YouTube, Instagram, Twitter, and the gaming platform Twitch were exposed last month by a data breach at a marketing firm that pairs online stars with top brands seeking product reviews and endorsements, according to researchers at the security firm UpGuard.

Attribution 1 Publication: gizmodo.com Author:
 Article Title: 12,000 Social Media Influencers, Mostly Women, Exposed by Marketing Firm Data Breach
 Article URL: <https://gizmodo.com/12-000-social-media-influencers-mostly-women-exposed-1822634002>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-08	Saginaw Valley State Universtiy	MI	1/24/2018	Electronic	Educational	Yes - Published #	4,949

On or about November 26, 2017, a password-protected university laptop was stolen from a University employee's private residence. On January 3, 2018, we determined that the stolen laptop may have contained your full name and Social Security number. (Number of Records Exposed per IN AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: Saginaw Valley State Universtiy
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/saginaw-valley-20180124.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-07	Rogin Nassau, LLC	CT	1/18/2018	Electronic	Business	Yes - Published #	268

Since completing our investigation and manual document review, which concluded on or about November 3, 2017, we concluded that an unauthorized third party accessed the email accounts at issue. Because we value our relationship with you, we wanted to notify you of this incident since your personal information was contained within one of the compromised email accounts, which included your full name and Social Security number. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: Rogin Nassau, LLC
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/rogin-nassau-20180118.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-06	City of Unalaska	AK	2/1/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

The City of Unalaska could be on the hook for nearly \$6,000 after unredacted copies of the mayoral recall petition were posted on Facebook. The city clerk has apologized to community members who had parts of their social security numbers released.

Attribution 1 Publication: kucb.org Author:
 Article Title: After City Mistakenly Releases Unredacted Petition, Clerk Offers To Cover Identity Theft Monitoring
 Article URL: <http://kucb.org/post/after-city-mistakenly-releases-unredacted-petition-clerk-offers-cover-identity-theft-monitoring>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-05	City of Keokuk	IA	2/4/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

The city said in a statement that an unauthorized party was able to obtain 2017 W-2 tax forms through the use of a "criminal phishing email."

Attribution 1 Publication: tspr.org / scmagazine.com Author:
 Article Title: Keokuk Data Breach Results in Stolen City Employee Information
 Article URL: <http://tspr.org/post/keokuk-data-breach-results-stolen-city-employee-information>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-04	CarePlus Health Plans	FL	2/5/2018	Paper Data	Medical/Healthcare	Yes - Published #	11,248

Explanation of benefits statements were mailed to its plan members on January 9 and January 16, 2018, although on January 17, CarePlus became aware that some of the statements had been sent to incorrect individuals. The EoB statements included names, addresses, dates of service, providers of services, the services that had been provided, CarePlus identification numbers and CarePlus health plan names.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
 Article Title: 11,200 CarePlus Health Plan Members Notified of PHI Breach
 Article URL: <https://www.hipaajournal.com/11200-careplus-health-plan-members-notified-phi-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-03	Robert Smith DMD, PC	TN	1/22/2018	Electronic	Medical/Healthcare	Yes - Published #	1,500

Smith Dental's internal computer servers were the target of a ransomware attack in November, 2017. While we have not seen evidence that any protected health information was accessed, copied or distributed, it is possible that some clinical, demographic, and financial information was compromised.

Attribution 1 Publication: [hhs.gov / databreaches.net](https://www.databreaches.net) Author:
Article Title: Robert Smith DMD, PC
Article URL: <https://www.databreaches.net/tn-smith-dental-notifies-hhs-of-ransomware-attacking-affecting-1500/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-02	Advanced Graphic Products, Inc. dba Advanced-Online	TX	2/1/2018	Electronic	Business	Yes - Published #	22,182

Advanced-Online learned on January 3, 2018 that certain personal information housed on the company's online platform may have been subject to unauthorized access. Advanced-Online and our cybersecurity and forensics firm believe that the following categories of information may have been compromised: name, address, username/email address, password, and payment card information (account number, expiration date, CVV number). (Number of Records exposed per NC AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Advanced Graphic Products, Inc. dba Advanced-Online
Article URL: https://oag.ca.gov/system/files/Sample_Notice_0.PDF

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180205-01	Ron's Pharmacy Services	CA	2/2/2018	Electronic	Medical/Healthcare	Yes - Published #	6,781

As part of this investigation, we determined that the employee's email account was subject to unauthorized access and certain emails were viewed as a result of the unauthorized individual(s) using software to crack the employee's email account password. On December 21, 2017, as part of Ron's Pharmacy's ongoing investigation, it was determined that the following information relating to you or your loved-one was accessed: your name, your internal account number at Ron's Pharmacy, prescription medication information, and payment adjustment information, which relates to credits made to your account.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Ron's Pharmacy Services
Article URL: https://oag.ca.gov/system/files/T927_v01.pdf_Prescription_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180201-04	Eastern Maine Medical Center	ME	2/1/2018	Electronic	Medical/Healthcare	Yes - Published #	660

The hospital has asked the FBI to help investigate the disappearance of the external hard drive, a 2-by-4 inch box that was connected to a desktop computer at the hospital's State Street facility. The hard drive, owned and operated by an outside vendor, contains patients' names, dates of birth, dates of their care, medical record numbers, one-word descriptions of their medical condition and images of their ablation, according to an EMMC press release.

Attribution 1 Publication: bangordailynews.com / databreaches.net Author:
Article Title: EMMC waited a month to alert patients of possible data breach
Article URL: <https://bangordailynews.com/2018/02/01/news/bangor/emmc-waited-a-month-to-alert-patients-of-possible-data-breach/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180201-03	HORNE LLP	MS	2/2/2018	Electronic	Medical/Healthcare	Yes - Published #	1,670

HORNE became aware of an email account breach on November 1, 2017 when it discovered the email account of an employee was being used to send phishing emails. On November 27, HORNE determined that some of those emails contained attachments that included PHI including names, birth dates, Medicaid ID numbers, patient account numbers, service dates, and Social Security numbers.

Attribution 1 Publication: hipaajournal.com / HORNE Notice of Da Author:
Article Title: HORNE LLP
Article URL: <https://www.hipaajournal.com/phishing-attack-exposes-forrest-general-hospital-patients-phi/>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180201-02	Kraus Associates, Inc. dba AK Associates	MA	1/26/2018	Electronic	Business	Yes - Published #	132

As you may remember from the call, on December 26 and 27, 2017, we learned that, on December 23, 2017, a third party installed ransomware known as Tastylock on an AK computer, which encrypted files on that computer. Specifically, the computer contained personnel records for 132 individuals who are current and former AK employees, or their spouses, dependents or beneficiaries, including name, date of birth, social security number, and bank account number(s). (Number of Records exposed per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
 Article Title: Kraus Associates, Inc. dba AK Associates
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/kraus-associates-20180126.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180201-01	Gillette Medical Imaging	WY	1/18/2018	Paper Data	Medical/Healthcare	Yes - Published #	4,476

Gillette Medical Imaging WY Healthcare Provider 4476 01/18/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: Gillette Medical 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
ITRC20180131-22	Pearlie Mae's Compassion and Care LLC	KS	1/25/2018	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Topeka, Kansas-based Pearlie Mae's Compassion and Care LLC recently agreed to pay an \$8,750 civil penalty after allegations that it had unsecured patient data in one of its office locations.

Attribution 1 Publication: healthitsecurity.com Author:
 Article Title: KS Healthcare Organization Fined over Unsecured Patient Data
 Article URL: <https://healthitsecurity.com/news/ks-healthcare-organization-fined-over-unsecured-patient-data>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180131-21	Allscripts	IL	1/31/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Last week, a ransomware attack against the EHR vendor Allscripts resulted in thousands of healthcare providers being unable to access patient data or use the e-prescription service.

Attribution 1 Publication: hipaajournal.com Author:
 Article Title: Class Action Lawsuit against Allscripts Filed following Ransomware Attack
 Article URL: <https://www.hipaajournal.com/class-action-lawsuit-allscripts-filed-following-ransomware-attack/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180131-20	VSA Partners, Inc.	IL	1/24/2018	Electronic	Business	Yes - Published #	455

We have discovered that a VSA employee's email account was accessed without authorization on December 1, 2017. (Information involved was redacted.) (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NY AG's office Author:
 Article Title: VSA Partners, Inc.
 Article URL: <http://ago.vermont.gov/blog/2018/01/24/vsa-partners-sbn-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180131-19	Pentair Aquatic Eco-Systems	FL	1/26/2018	Electronic	Business	Yes - Published #	239

On January 2, 2018, we identified unauthorized computer code added to the checkout page of our online store at <https://petairaescom>. The information on the checkout page that the code potentially accessed includes name, address, phone number, email address, payment card number, expiration date, and card security code (CVV). (Number of Records exposed per NY AG's office)



Attribution 1 Publication: VT AG's office / NH AG's office Author:
 Article Title: Pentair Aquatic Eco-Systems
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/pentair-aquatic-20180126.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180131-18	Vermont Health Connect	VT	1/30/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

It has come to our attention that another consumer was able view some of your payment information on the Vermont Health Connect (VHC) online portal. For a period of time beginning on December 26th, 2017 until discovery of the error on January 29th, 2018, one other consumer was able to view your recurring payment information that included your name, your bank name, and the last four digits of both the bank routing and your bank account number:

Attribution 1 Publication: VT AG's office Author:
 Article Title: Vermont Health Connect
 Article URL: <http://ago.vermont.gov/blog/2018/01/30/vermont-health-connect-ahs-sbn-consumers/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180131-17	National Registry of Emergency Medical Technicians (Nevada)	OH	1/25/2018	Electronic	Business	Yes - Published #	843

On December 14, 2017, NREMT learned that credentials belonging to a NDHHS employee were used without authorization on the NREMT certification web-based platform. While our investigation is ongoing, we determined on January 9, 2018, that the following information related to you may have been accessible to the unauthorized individual(s): first and last name, address information, and Social Security number. (Number of Records exposed per IN AG's office)

Attribution 1 Publication: MT AG's office Author:
 Article Title: National Registry of Emergency Medical Technicians (Nevada Department of Health and Human Services)
 Article URL: <https://dojmt.gov/wp-content/uploads/National-Registry-of-Emergency-Medical-Technicians.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180131-16	Goldleaf Partners	MN	1/26/2018	Electronic	Business	Yes - Published #	6,020

On or about October 31, 2017, we discovered that Goldleaf Partners ("Goldleaf") had become the target of a phishing email campaign that compromised an employee's email account credentials. While we currently have no evidence that the unauthorized individual or individuals actually accessed or acquired your information, we have confirmed that your <<ClientDef2 (data elements affected)>> were accessible to the unknown actor during this event. (Exposure number per NC AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180131-15	Nevro Corporation	CA	1/29/2018	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Nevro was recently the victim of a criminal break-in at our corporate headquarters in which several laptop computers were stolen. The categories of information varied by file or patient, but the data fields were limited to patient name, street address, birth date, procedure date, medical device identifiers (such as serial number), and contact information for the patient's physician or other medical provider.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Nevro Corporation
 Article URL: https://oag.ca.gov/system/files/Notification%20Letter%20-%20%20Nevro_0.pdf



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180131-14	Jeffrey Born CPA, Inc.	CA	1/26/2018	Electronic	Business	Yes - Unknown #	Unknown

On December 31, 2017, I learned that my office was physically broken into and that two password protected laptops were stolen. This may have included your: full name, birthdate, telephone number, address, Social Security number, all employment (W-2) and self-employment information, 1099 information (including account number if provided to my office), entity identification and income earned/amounts received from participation in S-Corp/partnership/LLC/trust, Affordable Care Act insurance data (your medical insurance policy number if you provided us with a Form 1095-A), and direct deposit bank account information (including account number and routing information if provided to my office).

Attribution 1 Publication: CA AG's office Author:
 Article Title: Jeffrey Born CPA, Inc.
 Article URL: https://oag.ca.gov/system/files/Born%20Notification_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180130-02	Pediatric Endocrinology and Diabetes Specialists	NV	1/18/2018	Electronic	Medical/Healthcare	Yes - Published #	1,021

The breach occurred on numerous days between 27 January 2014 until 7 February 2014. Information that appears to have been taken includes full name, date of birth, address, phone number along with email address, insurance payor, medical record number, diagnosis codes and clinical notes.

Attribution 1 Publication: hhs.gov / databreaches.net Author:
 Article Title: Pediatric Endocrinology and Diabetes Specialists
 Article URL: <http://www.thepeds.com/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180130-01	RBC (Travelocity)	TX	1/26/2018	Electronic	Banking/Credit/Financial	Yes - Published #	66,000

Travelocity immediately investigated and, on January 5, notified RBC that there had been unauthorized access to the Platform resulting in the likely exposure of payment card information for cards used on the Platform between October 3, 2017 and December 22, 2017. The investigation indicates that there likely was unauthorized access to your payment card number and CVV (the three- or four-digit security code on the back of the credit card). (Number of Records exposed per IN AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-15	Salvation Army of Augusta	GA	1/23/2018	Electronic	Business	Yes - Published #	570

Specifically, on November 7, 2017, The Salvation Army of Augusta was notified that the personal information provided by registrants for only The Salvation Army of Augusta's Auto Auction website (<http://www.salvationarmycars.com>) was accessible through a common search on the internet. Further, all information regarding the credit card information, including the panel code and CW, were deleted and purged from the website. Additionally, the website has since been completely shut down. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office Author:
 Article Title: Salvation Army of Augusta
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/salvation-army-20180123.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-14	Makeup Geek, LLC	MI	1/19/2018	Electronic	Business	Yes - Published #	2,385

The intrusion and accompanying data breach was discovered on or about December 18, 2017, following the discovery of suspicious code on Makeup Geek's website. After forensic analysis, it was determined that a computer hacker had managed to insert a hidden piece of malicious code into Makeup Geek's customer-facing web portal, which was able to intercept customer credit card information as it was being entered by the customer by means of a form of keystroke logging. (Number of Records exposed per NY AG's office)

Attribution 1 Publication: NH AG's office / MT AG's office / NY AG' Author:
Article Title: Makeup Geek, LLC
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/makeup-geek-20180119.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-13	Maplecrest Ford	NJ	1/19/2018	Electronic	Business	Yes - Published #	Unknown

On September 22, 2017, Maplecrest Ford learned that an employee was the victim of a phishing attack to his email account. Maplecrest Ford confirmed that the compromised email accounts contained name and either one or more of the following: Social Security number, credit card number, and/or driver's license number.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Maplecrest Ford
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/maplecrest-ford-20180119.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-12	KLX, Inc.	FL	1/24/2018	Electronic	Business	Yes - Published #	2,450

On December 1, 2017, a KLX laptop was stolen from one of our offices. Nonetheless, KLX undertook a further investigation that indicated, in mid-December 2017, that there was a probability that the laptop did contain one file containing the names, social security numbers, and salaries of certain employees. KLX' s further investigation confirmed this probability on January 2, 2017. (Exposure number per NC AG's office)

Attribution 1 Publication: NH AG's office / MT AG's office / NY AG' Author:
Article Title: KLX, Inc.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/klx-20180124.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-11	Hudson Structured Capital Management Ltd.	CT	1/10/2018	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Specifically, HSCM discovered recently that, for a period of approximately one week, an unauthorized person had acquired access to an email account of an HSCM employee. As a result of this unauthorized access, HSCM believes that this unauthorized person had the ability to access information about certain of its employees and investors - including potentially sensitive information such as names, addresses and social security numbers.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Hudson Structured Capital Management Ltd.
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/hudson-sstructured-20170110.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-10	Fidelity Investments (1/11/18)	MA	1/11/2018	Electronic	Banking/Credit/Financial	Yes - Published #	348

From November 24, 2017 to December 8, 2017, due to an error by Fidelity, information about your account(s) was inadvertently sent to a third-party which offers financial data analytics services to financial advisors, including financial advisors which do business with Fidelity. Information related to your account(s) included your name, Fidelity account number(s), Social Security number, date of birth, account balance and history. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Fidelity Investments (1/11/18)
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/fidelity-20180111.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-09	Kansas Secretary of State	KS	1/25/2018	Electronic	Government/Military	Yes - Unknown #	Unknown

Along with a bevy of personal information contained in documents that, according to a statement on the website, was intended to be public, the Kansas Secretary of State's website left exposed the last four digits of Social Security numbers (SSN4) belonging to numerous current and former candidates for office, as well as thousands—potentially tens of thousands—of high-ranking state employees at virtually ever Kansas government agency.

Attribution 1 Publication: gizmodo.com / databreaches.net Author:
Article Title: Kris Kobach's Office Leaks Last 4 Social Security Digits of Nearly Every Kansas Lawmaker and Thousands of State Employee
Article URL: <https://gizmodo.com/kris-kobach-s-office-leaks-last-4-social-security-digit-1822415622>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-08	Charlotte Housing Authority	NC	1/25/2018	Electronic	Government/Military	Yes - Published #	341

"Unfortunately, this information was provided before it was discovered that the request was made from a fraudulent account," Meachem wrote in an internal staff letter obtained by FOX 46. The W-2 forms contain Social Security numbers, addresses and private financial information. (Number of Records exposed per NY AG's office)

Attribution 1 Publication: Fox46charlotte.com / NY AG's office Author:
Article Title: Charlotte Housing Authority suffers data breach, hundreds impacted
Article URL: <http://www.fox46charlotte.com/news/local-news/exclusive-charlotte-housing-authority-suffers-data-breach-341-employ>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-07	Gourmesso	FL	1/24/2018	Electronic	Business	Yes - Unknown #	Unknown

Credit card information compromised. No additional information.

Attribution 1 Publication: ME AG's office Author:
Article Title: Gourmesso
Article URL: [Per ME AG's website update 1/26/18](http://www.megov.com/newsroom/2018/01/26/per-me-ag-s-website-update-1-26-18)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-06	San Diego County Office of Education	CA	1/25/2018	Electronic	Educational	Yes - Unknown #	Unknown

On December 5, 2017, a San Diego County Office of Education ("SDCOE") employee inadvertently sent an employee retirement contribution spreadsheet, containing employee name, Social Security number, and funding amount, to SDCOE's retirement

Attribution 1 Publication: MT AG's office Author:
Article Title: San Diego County Office of Education
Article URL: <https://dojmt.gov/wp-content/uploads/San-Diego-County-Office-of-Education.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-05	Steven Yang, D.D.S., Inc.	CA	1/26/2018	Electronic	Medical/Healthcare	Yes - Published #	3,202

On the morning of January 6, 2018, our dental office was burglarized and two laptops were stolen. Our investigation has determined that files contained on those devices may have included your name, address, social security number, health insurance number and other information regarding your dental care.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
Article Title: Steven Yang, D.D.S., Inc.
Article URL: https://oag.ca.gov/system/files/T875_v02%20-%20Notice_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-04	Member First Mortgage	MI	1/26/2018	Electronic	Banking/Credit/Financial	Yes - Published #	36,840

On December 21, 2017, we discovered that someone had gained unauthorized access to one of our employee's email accounts. The types of personal data that we believe were involved in the breach consisted of individuals' names, social security numbers, addresses, and mortgage loan account numbers. (Number of Records exposed per IN AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / IN AG' Author:
Article Title: Member First Mortgage
Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/member-first-20180126.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180129-03	Western Washington Medical Group Inc.	WA	1/12/2018	Paper Data	Medical/Healthcare	Yes - Published #	842

Western Washington Medical Group ("WWMG"), located in Everett, Washington, discovered that medical records and information for some of its patients may have been improperly disposed of on November 13, 2017. Information contained in the shred bins may have included names, addresses, diagnoses, medical history forms, appointment dates, medical history, and health care insurance billing information.

Attribution 1 Publication: [hhs.gov / databreaches.net](https://www.hhs.gov/databreaches.net) Author:
 Article Title: Western Washington Medical Group, 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
ITRC20180129-02	RGH Enterprises, Inc.	OH	1/22/2018	Paper Data	Medical/Healthcare	Yes - Published #	4,586

RGH Enterprises, Inc. OH Healthcare Provider 4586 01/22/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: [hhs.gov](https://www.hhs.gov) Author:
 Article Title: RGH Enterprises, 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
ITRC20180129-01	Rocky Mountain Women's Health Center, Inc.	UT	1/25/2018	Paper Data	Medical/Healthcare	Yes - Published #	1,166

Rocky Mountain Women's Health Center, Inc. UT Healthcare Provider 1166 01/25/2018 Improper Disposal Paper/Films

Attribution 1 Publication: [hhs.gov / NC AG's office](https://www.hhs.gov) Author:
 Article Title: Rocky Mountain Women's Health Center, Inc.
 Article URL: [Per FOIA request NC AG's office](#)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180125-01	Central States Southeast and Southwest Areas Health and Welfare Fund	IL	1/23/2018	Paper Data	Medical/Healthcare	Yes - Published #	634

Central States Southeast and Southwest Areas Health and Welfare Fund IL Health Plan 634 01/23/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: [hhs.gov](https://www.hhs.gov) Author:
 Article Title: Central States Southeast and Southwest Areas Health and Welfare Fund
 Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf?jsessionid=4865BEFDA4E9E18A73970E189367F552

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180124-08	Tennessee Valley Title Insurance Company	TN	1/9/2018	Electronic	Business	Yes - Published #	179

We recently learned that, on October 13, 2017, the email account of one of our employees was accessed by an unauthorized individual not affiliated with Tennessee Valley. In that regard, it is possible that the individual may have had access to email(s) that were in the compromised account and which contained information about you, including your name, address, Social Security number, date of birth, driver's license or government identification card number, account number, or debit or credit card number. (Exposure number per NY AG's office)

Attribution 1 Publication: [NH AG's office / NY AG's office](#) Author:
 Article Title: Tennessee Valley Title Insurance Company
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/tennessee-valley-20180109.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180124-07	Florida Secretary of State (Crosscheck)	FL	1/22/2018	Electronic	Government/Military	Yes - Published #	945

Partial Social Security numbers for nearly 1,000 Kansas voters were released publicly by Florida after Secretary of State Kris Kobach's office provided the data as part of a program that looks for double voter registrations.

Attribution 1 Publication: [kansascity.com](#) Author: _____
Article Title: Private info for hundreds of Kansas voters exposed by Florida
Article URL: <http://www.kansascity.com/news/politics-government/article196029319.html>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180124-06	Questar Assessment (multiple school districts in multiple states)	MN	1/22/2018	Electronic	Business	Yes - Unknown #	Unknown

Questar's preliminary analysis found that an unauthorized user viewed student assessment records between Dec. 31, 2017 and Jan. 1 from Tupelo Middle School, Tupelo High School and Jefferson County Junior High School. The unauthorized viewer gained access to student names, Mississippi student identification numbers, grade levels, teacher names and test results. One student record viewed contained demographic data.

Attribution 1 Publication: NYS Education Department Author: _____
Article Title: State Education Department Announces Breach of Data Held by Vendor Questar
Article URL: <http://www.nysed.gov/news/2018/state-education-department-announces-breach-data-held-vendor-questar>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180124-05	National Stores, Inc.	CA	1/22/2018	Electronic	Business	Yes - Published #	609,064

On December 22, 2017, National Stores received an alert that its point-of-sale systems were affected by malware, and that customer payment card information may have been accessed without authorization. The affected payment card information may have included names, card numbers, card expiration dates, and security codes. (Exposure number per IN AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author: _____
Article Title: National Stores, Inc.
Article URL: [http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294960%20\(1\).pdf](http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2018/itu-294960%20(1).pdf)

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180124-03	DJO, LLC	CA	1/10/2018	Paper Data	Medical/Healthcare	Yes - Published #	1,203

On September 25, 2017 we discovered that the DJO Global Patient Product Agreement form may have been lost in transit. The form may have contained your name, address, phone number, date of birth, physician name, physician location, product information, product order date, date of injury, diagnosis code(s), health plan information, and health plan identification number (which may incorporate your social security number).

Attribution 1 Publication: [hhs.gov / DJO website](#) Author: _____
Article Title: Privacy Incident Affecting Paper Records
Article URL: <http://www.djoglobal.com/corporate-info/privacy-incident-faqs>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180124-02	Alicia Ann Oswald	CA	1/9/2018	Electronic	Medical/Healthcare	Yes - Published #	800

Alicia Ann Oswald CA Healthcare Provider 800 01/09/2018 Unauthorized Access/Disclosure Email

Attribution 1 Publication: [hhs.gov](#) Author: _____
Article Title: Alicia Ann Oswald
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: 7/2/2018

Page 128 of 134

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180124-01	High Plains Surgical Associates	WY	1/15/2018	Paper Data	Medical/Healthcare	Yes - Published #	607

High Plains Surgical Associates WY Healthcare Provider 607 01/15/2018 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
 Article Title: High Plains Surgical 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
ITRC20180123-07	Hallmark Home Mortgage	IN	1/12/2018	Electronic	Banking/Credit/Financial	Yes - Published #	2,816

On November 17, 2017, we learned that former employees may have had unauthorized access to certain of our customers' personal information after leaving our employment. We conducted a thorough review and determined that the information that the former employees may have had unauthorized access to includes information from your loan or loan application, which would include information you submitted to Hallmark or Hallmark obtained on its own, including your name<variable data elements>. Type of information exposed was not disclosed. (Number of Records exposed per IN AG's office)

Attribution 1 Publication: VT AG's office Author:
 Article Title: Hallmark Home Mortgage
 Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Hallmark%20Home%20Mortgage%20SBN%20to%20Co

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180123-06	Monticello Central School District	NY	1/17/2018	Electronic	Educational	Yes - Published #	2,598

Regrettably, we are writing to inform you of a sophisticated e-mail phishing attack that we believe occurred on or around November 1, 2017. The incident may have resulted in unauthorized access to your personal information, which included your name, address, Social Security number and date of birth. (Number of Records exposed per IN AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office Author:
 Article Title: Monticello Central School District
 Article URL: <https://www.doi.nh.gov/consumer/security-breaches/documents/monticello-20180112.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180123-05	Westminster Ingleside King Farm Presbyterian Retirement Communities	MD	1/19/2018	Electronic	Business	Yes - Published #	9,769

A malware infection at Westminster Ingleside King Farm Presbyterian Retirement Communities has potentially enabled the attackers to gain access to the protected health information of thousands of its residents. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / ME AG's office / hipaajo Author:
 Article Title: Malware Causes 5,200-Record Data Breach at DC Assisted Living Facility
 Article URL: <https://www.hipaajournal.com/?s=westminster>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180123-04	Arthur Ventures Management, LLC	ND	1/12/2018	Electronic	Business	Yes - Published #	210

On December 15, 2017, we learned that certain of your personal information could have been viewed as part of an email account compromise. You are receiving this notice because we recently learned that certain of your personal information could have been accessed, including your name, Social Security number and, for some individuals, driver's license number. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NY AG's office Author:
 Article Title: Arthur Ventures Management, LLC
 Article URL: <https://dojmt.gov/wp-content/uploads/Arthur-Ventures-Management-LLC.pdf>



ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180123-03	Pension Fund of the Christian Church	IN	1/16/2018	Electronic	Business	Yes - Published #	20,996

As we previously communicated to our membership, Pension Fund recently became aware of a potential unauthorized access to one of its legacy servers. The legacy server file included some members' names, dates of birth, Social Security numbers, and member identification number (PIN). The laptop contained members' names, date of birth, addresses, account numbers, Social Security numbers, and PIN. (Number of Records exposed per IN AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / OR AG Author:
 Article Title: Pension Fund of the Christian Church
 Article URL: https://oag.ca.gov/system/files/PFR%20Standard%20Notification%20Letter%20Sample%201_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180123-02	American Golf Corporation	CA	1/17/2018	Electronic	Business	Yes - Published #	1,099

Based upon the vendor's investigation, it appears that an unauthorized individual was able to gain access to portions of our website and install malicious software on the website servers designed to capture payment card information as it was being entered on the site. We believe that the incident could have affected certain information (including name, address, phone number, email address, payment card account number, expiration date, and verification code) of individuals who booked a tee time on the website between December 12, 2017 and December 15, 2017. (Number of Records exposed per NY AG's office)

Attribution 1 Publication: CA AG's office / NY AG's office Author:
 Article Title: American Golf Corporation
 Article URL: https://oag.ca.gov/system/files/Sample%20Notice_20.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180123-01	Mindlance	NJ	1/19/2018	Electronic	Business	Yes - Published #	3,085

Certain Mindlance confidential and proprietary information was stolen on or about December 28, 2017. On December 29, 2017, the stolen information was e-mailed to several current corporate Mindlance employees. An attachment to the December 29, 2017 e-mail contained the name and Social Security number, related only to a limited number of Mindlance employees. (Number of Records exposed per NY AG's office)

Attribution 1 Publication: CA AG's office / ME AG's office / NY AG Author:
 Article Title: Mindlance
 Article URL: https://oag.ca.gov/system/files/California%20Template%20Notification%20%28152381521_1%29_0.PDF

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180119-08	Guaranteed Rate, Inc.	IL	1/12/2018	Electronic	Business	Yes - Published #	187,788

On or around September 13, 2017, we confirmed a limited number of company email accounts were accessed by unknown actors as the result of these phishing attacks. Our investigation indicates that the following types of your personal information were viewed or downloaded by the unknown actors: Social Security number and name. (Number of Records exposed per IN AG's office)

Attribution 1 Publication: VT AG's office / CA AG's office / MT AG' Author:
 Article Title: Guaranteed Rate, Inc.
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/guaranteed-rate-20180112.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180119-07	PharMerica / Onco360 / CareMed Specialty Pharmacy	KY	1/12/2018	Electronic	Medical/Healthcare	Yes - Published #	53,173

On November 14, 2017, we discovered suspicious activity involving an employee's email account. On November 30, 2017, the forensic investigation determined that an unauthorized user appeared to have gained access to email accounts of three employees. A detailed review of the impacted e-mail accounts was performed and on January 8, 2018, we determined that the emails in those e-mail accounts contained your name and Social Security number and may have potentially contained your address, medication and clinical information, and health insurance information.



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

Report Date: 7/2/2018

Page 130 of 134

Attribution 1 Publication: VT AG's office / hhs.gov / ME AG's office Author:
 Article Title: PharMerica / Onco360 / CareMed Specialty Pharmacy
 Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/pharmerica-20180112.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180119-06	Pedes Orange County	CA	1/12/2018	Electronic	Medical/Healthcare	Yes - Published #	917

On November 14, 2017, we learned that a physician from another medical group in the facility accessed our Pedes electronic medical records database without permission and disclosed the database materials to their attorney. Our investigation has determined that the database contained some of your personal health information, including your name, medical diagnosis, medical treatments, dates of medical service, and other treatment related information.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
 Article Title: Pedes Orange County
 Article URL: https://oag.ca.gov/system/files/Pedes%20Adult%20CA%20Notice_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180119-05	NHS, Inc.	CA	1/10/2018	Electronic	Business	Yes - Unknown #	Unknown

On December 29, 2017, NHS's third-party e-commerce vendor discovered that our website was the target of a cybersecurity attack aimed at acquiring customer credit card information. The information discovered may include your name, address, credit card information, expiration date and security code (CVV).

Attribution 1 Publication: CA AG's office Author:
 Article Title: NHS, Inc.
 Article URL: https://oag.ca.gov/system/files/Notice%20of%20Breach_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180119-04	Kaiser Foundation Health Plan (9/21/17)	CA	1/19/2018	Paper Data	Medical/Healthcare	Yes - Published #	638

On 9/21/17, we discovered that a letter intended for you was inadvertently mailed to another Kaiser Permanente member. You may have also received a similar letter intended for another KP member. The letter intended for you referenced Kaiser Permanente's Liver Care Program and contained your first and last name, and medical record number.

Attribution 1 Publication: hhs.gov / CA AG's office Author:
 Article Title: Kaiser Foundation Health Plan (9/21/17)
 Article URL: https://oag.ca.gov/system/files/FINAL%20Member%20Notification%20Letter_10.10.17_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180117-04	Multnomah Athletic Club	OR	1/11/2018	Electronic	Business	Yes - Published #	18,632

On December 5, 2017, we learned that multiple shredding bins located on the premises of the Multnomah Athletic Club were stolen on December 2, 2017 by multiple unknown individuals. It is possible, however, that one or more of the bins contained your name, address, Social Security number, passport, driver's license number, and/or bank account information (routing and account numbers). (Exposure number per NY AG's office)

Attribution 1 Publication: OR AG's office / NH AG's office / NY AG Author:
 Article Title: Multnomah Athletic Club
 Article URL: <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1161073650>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180117-02	Agency for Health Care Administration	FL	1/5/2018	Electronic	Medical/Healthcare	Yes - Published #	30,000

A phishing attack on an employee at Florida's Agency for Health Care Administration resulted in the exposure of sensitive information on 30,000 Medicaid patients, the agency said in a Saturday notification. The IG's initial review indicated that the names, Medicaid ID numbers, birth dates, diagnoses, Social Security numbers, addresses, and medical conditions of up to 30,000 recipients "were accessed in part or full."

Attribution 1 Publication: [scmagazine.com / hhs.gov](http://scmagazine.com/hhs.gov) Author:
Article Title: Breach possibly exposed sensitive data on up to 30K Florida Medicaid recipients
Article URL: <https://www.scmagazine.com/breach-possibly-exposed-sensitive-data-on-up-to-30k-florida-medicaid-recipients/article/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180116-10	MD Medical Spa and Wellness Center	MA	1/15/2018	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Medical records were found dumped in New Bedford, sparking concern in the community. Private information like social security numbers and licenses are printed in the files, New Bedford Live reported.

Attribution 1 Publication: [turnto10.com / databreaches.net](http://turnto10.com/databreaches.net) Author:
Article Title: Medical records found dumped in New Bedford
Article URL: <http://turnto10.com/news/local/medical-records-found-dumped-in-new-bedford>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180116-08	Palomar Medical Center Escondido	CA	1/8/2018	Electronic	Medical/Healthcare	Yes - Published #	1,309

More than 1,300 patients of Palomar Medical Center Escondido are being notified that a former nurse viewed their medical records without authorization while they were receiving treatment at the hospital. The information viewed was limited to names, dates of birth, genders, medical record numbers, treatment locations, diagnoses, allergies, and medications for 1,309 patients

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 1,300 Patients' Medical Records Viewed Without Authorization by Palomar Health Nurse
Article URL: <https://www.hipaajournal.com/1300-patients-medical-records-viewed-without-authorization-palomar-health-nurse/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180116-05	Northeast Arc	MA	1/5/2018	Electronic	Business	Yes - Published #	1,823

On December 8, 2017, Northeast Arc discovered that an employee payroll file was inadvertently accessible to users of the Northeast Arc information systems, between March 2017 to December 2017. The employee payroll file contained the following information about you: name, Social Security number, financial account information, and routing information. (Exposure number per NC AG's office)

Attribution 1 Publication: VT AG's office / ME AG's office / NH AG' Author:
Article Title: Northeast Arc
Article URL: <https://www.doj.nh.gov/consumer/security-breaches/documents/northeast-arc-20180105.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180116-04	talentReef, Inc.	CO	1/10/2018	Electronic	Business	Yes - Published #	11,603

On November 29, 2017, it was discovered that an unauthorized individual may have gained access to an employee's email account which had messages containing some of your personal information. As part of our investigation, we identified a message containing some personal information, including your name, address, <<affected data>> Type of information exposed was not disclosed. (Number of Records exposed per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180116-03	Broward College	FL	1/10/2018	Electronic	Educational	Yes - Published #	44,000

On or about August 3, 2017, certain Broward College employees received a spam phishing email to their Broward College email accounts. Broward College also immediately initiated an investigation, with the assistance of a third-party forensic investigator, to determine what personal information, if any, was subject to unauthorized access or acquisition. Type of information exposed was not disclosed. (Number of Records exposed per NC AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180116-02	Alton Lane Inc.	VA	1/10/2018	Electronic	Business	Yes - Published #	1,208

In late November, 2017, Alton Lane received notice that in or about November of 2016, malicious code was injected into its information technology systems. Because of the nature of the breach, it is possible that some of your personal information — which may include your name, billing address, shipping address, and phone number, as well as the credit card information for the account you used to make a purchase from Alton Lane — may have been compromised. (Number of Records exposed per NC AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180116-01	Jason's Deli	TX	1/12/2018	Electronic	Business	Yes - Published #	3,400,000

From our initial investigation findings, criminals deployed RAM-scraping malware on a number of our point-of-sales (POS) terminals at various corporate-owned Jason's Deli restaurants starting on June 8, 2017. While this information varies from card issuer to card issuer, full track data can include the following: cardholder name, credit or debit card number, expiration date, cardholder verification value, and service code

Attribution 1 Publication: jasonsdeli.com / MT AG's office / VT AG' Author:
Article Title: Jason's Deli
Article URL: <https://www.jasonsdeli.com/data-breach>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180112-03	Penn Medicine	PA	1/2/2018	Electronic	Medical/Healthcare	Yes - Published #	1,050

Philadelphia-based Penn Medicine mailed letters to roughly 1,000 patients, alerting them to a potential compromise of their personal information after an unencrypted laptop was stolen from the hospital, a spokesperson told Becker's Hospital Review. The laptop contained a file with patient names, dates of birth, medical records and patient account numbers, and some demographic and medical information.

Attribution 1 Publication: hhs.gov / beckershospitalreview.com Author:
Article Title: Stolen computer at Penn Medicine compromises 1k patient records
Article URL: <https://www.beckershospitalreview.com/cybersecurity/stolen-computer-at-penn-medicine-compromises-1k-patient-rec>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180112-02	Oklahoma State University Center for Health Sciences	OK	1/5/2018	Electronic	Medical/Healthcare	Yes - Published #	279,865

On Nov. 7, 2017, we learned an unauthorized third party had gained access to folders on the OSUCHS computer network," the notification letter says. These folders stored Medicaid patient billing information.

Attribution 1 Publication: hhs.gov / healthcareinfosecurity.com Author:
Article Title: 'Hacking Incident' Impacts Nearly 280,000 Medicaid Patients
Article URL: <https://www.healthcareinfosecurity.com/hacking-incident-impacts-nearly-280000-medicaid-patients-a-10587?rf=2018-0>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180111-12	Cetera Advisors LLC (1/8/18)	CO	1/8/2018	Electronic	Business	Yes - Published #	1,260

On or about November 8, 2017, Cetera learned that an unauthorized individual may have gained access to an employee's email account. As part of our investigation, we identified a message containing some personal information, including your name, address, and Social Security number that appears to have been sent outside our organization. (Number of Records exposed per NC AG's office)

Attribution 1 Publication: MT AG's office / ME AG's office / MD A Author:
Article Title: Cetera Advisors LLC
Article URL: <https://dojmt.gov/wp-content/uploads/Cetera-Advisors-LLC.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180111-11	Columbia Falls School District	MT	1/5/2018	Electronic	Educational	Yes - Unknown #	Unknown

This notice pertains to the cyber extortion threat that Columbia Falls experienced in September 2017. The District Administration Office maintained a database containing employee records that included your name and Social Security number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180111-10	Montana State University Billings	MT	1/12/2018	Electronic	Educational	Yes - Unknown #	Unknown

On November 11, 2017, we learned that items, including an athletic department laptop, were stolen that same day from an employee's vehicle while traveling. Our investigation determined some of your information may have been contained on the laptop, including your name, health insurance information, date of birth, social security number and limited health information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180111-05	Rea.deemingBeauty, Inc. dba beautyblender	PA	1/5/2018	Electronic	Business	Yes - Published #	18,133

The website hosting company discovered what it believed was a form of malicious code on our site on October 26, 2017 which it then removed. On November 27, 2017, the forensic investigator confirmed that the malware inserted into our website collected certain payment card information used at checkout. (Number of Records exposed per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NY AG' Author:
Article Title: BeautyBlender / Rea.deemingBeauty, Inc.
Article URL: <https://dojmt.gov/wp-content/uploads/Beautyblenders.pdf>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180111-04	DHS Office of the Inspector General Case Management System	DC	1/3/2018	Electronic	Government/Military	Yes - Published #	247,167

A data breach at the Department of Homeland Security exposed the personally identifiable information on more than 240,000 current and former DHS employees, the department said Wednesday. Information exposed included Social Security numbers, dates of birth, positions, grades and duty stations. .

Attribution 1 Publication: cnet.com Author:
Article Title: Homeland Security breach exposes data on 240,000 employees
Article URL: <https://www.cnet.com/news/homeland-security-breach-exposes-data-on-240000-employees/>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180111-03	Charles River Medical Associates	MA	1/8/2018	Electronic	Medical/Healthcare	Yes - Published #	9,378

Charles River Medical Associates says it lost a portable hard drive believed to contain personal information and x-ray images of everyone who received a bone density scan at its Framingham radiology lab within the past eight years. The hard drive stored names, dates of birth, patient identification numbers and bone density scan images dating back to 2010.

Attribution 1 Publication: wickedlocal.com / hhs.gov Author:
 Article Title: Charles River Medical Associates
 Article URL: <http://www.wickedlocal.com/news/20180108/framingham-radiology-lab-loses-medical-records-of-9300-people>

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20180111-01	Flagship Facility Services, Inc.	CA	1/5/2018	Electronic	Business	Yes - Unknown #	Unknown

On or about December 5, 2017, Flagship determined that a company-owned HP Elite Laptop ("Laptop") was missing from 190 Jefferson, Menlo Park, California 94025. Type of information exposed was not disclosed.

Attribution 1 Publication: CA AG's office Author:
 Article Title: Flagship Facility Services, Inc.
 Article URL: https://oag.ca.gov/system/files/FlagShip%20Data%20Breach%20Notification%20Letter%20January%202018_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20120228-03	Wallace Community College	AL	2/24/2018	Electronic	Educational	Yes - Unknown #	Unknown

The Virtual SEPO blog reports that Wallace Community College in Alabama was hacked. Included in the data dump/proof of hack were 8 usernames, e-mail addresses, and passwords and a second table with 276 usernames, passwords, and full names. The passwords appear to be MD5 and were easily cracked using an online tool.

Attribution 1 Publication: databreaches.net Author:
 Article Title: Wallace Community College hacked
 Article URL: <https://www.databreaches.net/al-wallace-community-college-hacked/>

2018 Breaches Identified by the ITRC as of:	7/2/2018
--	-----------------

Total Breaches:	668
Records Exposed:	22,408,258

The Identity Theft Resource Center breach database is updated daily and published to our website weekly. A US-based breach, as identified by our current process, is considered public when one of these occur:

1) Published by a credible source (Sources include Offices of the Attorney General, and established media – TV news, radio, newspapers)

2) A letter notifying a potential victim has been received

ITRC will provide attribution of the source and include the relevant data to the extent that has been made public in our findings. If the number of records is not made publicly available, ITRC will note that in the report as "unknown" indicating we do not have the specifics of the actual number impacted. Identity Theft Resource Center reserves the right to make an educated estimate to the potential of impact based on our knowledge and understanding of the specifics of the policies of the reporting entity..



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.