ITRC Breach ID	Company or Agency	State	Published Date	Breach Category	Records Exposed?	Records Reported
ITRC20180611-23	**St. Mary's Health, Inc. dba St. Vincent Evansville**	IN	6/5/2018	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 Category	Records Exposed?	Records Reported
ITRC20180611-22	**Village of Wellington (Click2Gov)**	FL	6/7/2018	Government/Military	Yes - Unknown #	**Unknown**

Wellington's billing vendor, Superion, notified the village Wednesday that the company found "vulnerabilities in their software" for the Click2Gov system after customers reported potential unauthorized charges to credit cards used to pay utility bills, according to a news release.

Attribution 1
Publication: palmbeachpost.com Author:
Article Title: Wellington: Potential data breach may have exposed information
Article URL: https://www.palmbeachpost.com/news/local/wellington-potential-data-breach-may-have-exposed-information/3A03rMf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Category	Records Exposed?	Records Reported
ITRC20180611-21	**Blue Cross Blue Shield of Illinois (Dane Street)**	IL	6/6/2018	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 Category	Records Exposed?	Records Reported
ITRC20180611-18	**University of Utah Health**	UT	6/2/2018	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 Category	Records Exposed?	Records Reported
ITRC20180611-17	**Capitol Anesthesiology**	TX	6/1/2018	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 Category	Records Exposed?	Records Reported
ITRC20180611-16	**RISE Wisconsin, Inc.**	WI	6/7/2018	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 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 Category	Records Exposed?	Records Reported
ITRC20180611-15	**Terros Health**	AZ	6/8/2018	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 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-potentiall

ITRC Breach ID	Company or Agency	State	Published Date	Breach Category	Records Exposed?	Records Reported
ITRC20180611-13	**Forever 21 (Willis Towers Watson)**	CA	6/1/2018	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 Category	Records Exposed?	Records Reported
ITRC20180611-12	**Hair Free Forever**	CA	6/3/2018	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 Category	Records Exposed?	Records Reported
ITRC20180611-11	**Edward D. Jones & Co, L.P. (PricewaterhouseCoopers LLP)**	MO	6/4/2018	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.
Article URL: https://oag.ca.gov/system/files/LGL-11189-A_FINAL_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Category	Records Exposed?	Records Reported
ITRC20180611-10	**PLAE, Inc.**	CA	6/4/2018	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 Author:
Article Title: PLAE, Inc.
Article URL: https://oag.ca.gov/system/files/PLAE%20Notification%20Letter%20-%20052918%20FINAL_for%20state%20regulators_

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

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 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 Category	Records Exposed?	Records Reported
ITRC20180611-08	**Aimbridge Hospitality Holdings, LLC**	TX	6/7/2018	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 Category	Records Exposed?	Records Reported
ITRC20180611-07	**Systeme Software, Inc.**	PA	6/7/2018	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 Category	Records Exposed?	Records Reported
ITRC20180611-06	**Manduka**	CA	6/8/2018	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 Category	Records Exposed?	Records Reported
ITRC20180611-04	**Elmcroft Senior Living, Inc.**	OR	6/1/2018	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 Author:
Article Title: Elmcroft Senior Living, Inc.
Article URL: https://oag.ca.gov/system/files/Elmcroft%20-%20Ad%20-%206.1.18%20final_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Category	Records Exposed?	Records Reported
ITRC20180611-03	**Transamerica**	IA	6/1/2018	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 Category	Records Exposed?	Records Reported
ITRC20180604-07	**John A. Moran Eye Center at the University of Utah**	UT	6/2/2018	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 Category	Records Exposed?	Records Reported
ITRC20180604-04	**TicketFly, Inc.**	CA	6/1/2018	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

Monthly Breaches as of:	6/12/2018

Total Breaches:	19
Records Exposed:	8,776

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.