ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151229-07	SAS Safety Corporation	CA	12/24/2015	Electronic	Business	Yes - Unknown #	Unknown

Based upon the Company's investigation, the maiware was present from September 23, 2015 to December 8, 2013 and potentially exposed certain personal information of one resident that was inputted by that customer. The personal information that was potentially affected by the incident includes: customer name, address, credit or debit card number, payment card expiration date and the card's CVV security number. Additionally, the customer's logon identification and password for the website may have been affected. The Company does not collect customers' social security or driver's license numbers and that data was in no way affected by the incident.

Attribution 1 Publication: NH AG's office Author:
Article Title: SAS Safety Corporation
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/sas-safety-20151224.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151229-06	AllMed / Central Alabama Primary Care Specialists	AL	12/21/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Medical records were found Monday in an open air dumpster behind a former medical clinic called AllMed on Eastchase Parkway near Minnie Brown Road in east Montgomery. The records included prescriptions, lab results, names of patients and their birthdays -- all considered Private Health Information under HIPAA privacy laws.

Attribution 1 Publication: WTVM. Com / databreaches.net Author:
Article Title: Medical records found in dumpster in east Montgomery
Article URL: http://www.wtvm.com/story/30804533/exposed-medical-records-found-in-dumpster-in-east-montgomery

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151229-05	Cottonwood Comfort Dental	NM	12/26/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

An Albuquerque man said he found hundreds of medical records dumped on the West Mesa. The medical records include people's addresses, insurance information and social security numbers.

Attribution 1 Publication: databreaches.net / KRQE Author:
Article Title: New Mexican dental patients' records found dumped along West Mesa
Article URL: http://www.databreaches.net/new-mexican-dental-patients-records-found-dumped-along-west-mesa/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151229-04	Oregon Department of Veterans' Affairs	OR	12/29/2015	Paper Data	Government/Military	Yes - Published #	967

The Oregon Department of Veterans' Affairs says the personal information of hundreds of veterans may have been compromised.

Attribution 1 Publication: databreaches.net Author:
Article Title: Personal Info On Hundreds Of Oregon Veterans Compromised
Article URL: http://www.databreaches.net/personal-info-on-hundreds-of-oregon-veterans-compromised/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151229-03	Quincy Credit Union	MA	12/29/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Authorities continue to investigate a security breach at the Quincy Credit Union, a breach that gave hackers access to hundreds of accounts.

Attribution 1 Publication: BostonCBSLocal.com / databreaches.ne Author: Jim Smith
Article Title: Security Breach At Quincy Credit Union Investigated
Article URL: http://boston.cbslocal.com/2015/12/28/security-breach-at-quincy-credit-union-investigated/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151229-02	**Home Delivery Incontinence Supplies**	MO	12/28/2015	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

We began investigating the incident immediately upon learning of it on November 30, 2015. Based upon our investigation, it appears the incident occurred when harmful computer code, known as "malware," was inserted onto the shopping cart checkout software on our website without our authorization and despite the security features we have in place. This malware may have accessed customer information as it was input by customers during the checkout process.

Attribution 1 Publication: VTAG's office Author:
Article Title: Home Delivery Incontinence Supplies
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/HDIS%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151229-01	**Washington Township Health Care District**	WA	10/8/2015	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

Breach posted on AG website with no breach notification letter.

Attribution 1 Publication: CA AG's Office Author:
Article Title: Washington Township Health Care District
Article URL: https://oag.ca.gov/ecrime/databreach/reports/sb24-59419

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151228-07	**Belgrade Regional Health Center**	ME	12/18/2015	Paper Data	Medical/Healthcare	Yes - Published #	**854**

A physician's assistant leaving the Belgrade Regional Health Center warranted a letter being sent to patients to tell them about the impending change in personnel; however, that letter also resulted in a breach of 854 patients' Protected Health Information (PHI). The mailing took place on October 21, 2015 and patients first started notifying the health center of the error two days later when the letters started to be received.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Belgrade Regional Health Center
Article URL: http://www.hipaajournal.com/mailing-error-results-in-phi-exposure-of-belgrade-regional-health-center-patients-8238/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151228-06	**Physicians Health Plan of Northern Indiana**	IN	12/24/2015	Paper Data	Medical/Healthcare	Yes - Published #	**1,708**

Physicians Health Plan of Northern Indiana has alerted some of its Indigo members about a breach of a limited amount of their Protected Health Information (PHI) after an error was made mailing their billing statements. The breach involved multiple billing statements being sent on December 8, 2015, some of which were intended for other health plan subscribers. The mistake has been attributed to human error.

Attribution 1 Publication: hipaajournal.com / databreaches.net Author:
Article Title: MAILING ERROR EXPOSES PHI OF PHP HEALTH PLAN SUBSCRIBERS
Article URL: http://www.hipaajournal.com/mailing-error-exposes-phi-of-php-health-plan-subscribers-8236/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151228-05	**Voter Registration Database**	US	12/28/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Researcher Chris Vickery, who this month found myriad databases left open to all and sundry, told FORBES he has his hands on all 300GB of voter data, which includes names, home addresses, phone numbers, dates of birth, party affiliations, and logs of whether or not they had voted in primary or general elections. The data appears to date back to 2000. It does not contain financial data or social security numbers.

Attribution 1 Publication: Forbes.com Author:
Article Title: 191 Million US Voter Registration Records Leaked In Mystery Database
Article URL: http://www.forbes.com/sites/thomasbrewster/2015/12/28/us-voter-database-leak/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151228-04	**HealthSouth Rehabilitation Hospital of Round Rock**	TX	12/23/2015	Electronic	Medical/Healthcare	Yes - Published #	**1,359**

HealthSouth Rehabilitation Hospital of Round Rock (Texas) is notifying individuals that some medical and personal information may have been lost when an employee's laptop was stolen.

Attribution 1 Publication: HealthSouth Hospital of Round Rock we Author:
Article Title: Rehabilitation Hospital in Round Rock Notifies Individuals of Possible Theft of Health Data
Article URL: http://www.healthsouthroundrock.com/en/news-listing/2015-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151228-03	**Hyatt Hotels**	IL	12/27/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Hyatt Hotels recently detected malware on the computer system that processes payments for its hotels, The Guardian reports. It's not clear at this point whether any customer data was actually stolen, how long the malware was present on the system, or how many of the company's 627 properties in 52 countries may be affected.

Attribution 1 Publication: esecurityplanet.com Author: Jeff Goldman
Article Title: Hyatt Hotels Hit by Credit Card Breach
Article URL: http://www.esecurityplanet.com/network-security/hyatt-hotels-corporation-suffers-credit-card-breach.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151228-02	**Acclaim Technical Services, Inc.**	CA	12/23/2015	Electronic	Business	Yes - Unknown #	**Unknown**

We recently learned that Acclaim Technical Services, Inc., (“ATS”) was the target of a malicious, state-sponsored cyber intrusion which resulted in the theft of certain background investigation and other records containing personal information. You are receiving this letter because we have determined that your personal information may have been included in a background investigation form that was compromised during the incident.

Attribution 1 Publication: CA AG's office / VT AG's office Author:
Article Title: Acclaim Technical Services, Inc.
Article URL: https://oag.ca.gov/system/files/ATS%20Sample%20Letter%201_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151228-01	**Matson Navigation Company / Horizon Lines**	CA	12/7/2015	Electronic	Business	Yes - Unknown #	**Unknown**

The device was first identified as potentially missing on or about December 7, 2015 and appears to have been lost between November 9 and December 7, 2015. While our investigation is ongoing, we have determined that among the electronic files contained on the device were ones containing individualized information of mariners who have served aboard vessels operated by Horizon Lines since the year 2000. Accordingly, we believe your personal information may have been contained on the missing device. The personal information on the device included names, birth dates, addresses, telephone numbers, emergency contact information, Social Security numbers, and in some cases bank account and routing numbers, photocopies of passports, Transportation Worker Identification Credentials (TWIC), Merchant Mariner Documents (MMD) and Merchant Mariner

Attribution 1 Publication: CA AG's office / VT AG's office Author:
Article Title: Matson Navigation Company / Horizon Lines
Article URL: https://oag.ca.gov/system/files/ACID_PRINTERPROOFS_20151222_matson501_2_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151222-07	**Uncle Maddio's Pizza Joint**	GA	12/22/2015	Electronic	Business	Yes - Published #	**972**

Screencaps provided to DataBreaches.net revealed that 972 former and current employees had their name, address, phone number, hire and termination date (if no longer employed), pay rate, and Social Security numbers in plain text stored in the database. Not all employees had SSNs in the database, which humorously, has directories called “Kerrigan” and “Sarah.”

Attribution 1 Publication: databreaches.net Author:
Article Title: Database leak exposes Uncle Maddio’s employees’ and customers’ info
Article URL: http://www.databreaches.net/database-leak-exposes-uncle-maddios-employees-and-customers-info/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151222-06	Alliance Health	UT	12/22/2015	Electronic	Medical/Healthcare	Yes - Published #	Unknown

Like many other sites DataBreaches.net has reported on recently, Alliance Health had a configuration error in its MongoDB Database installation.

Attribution 1 Publication: databreaches.net Author:
Article Title: Misconfigured database may have exposed 1.5 million individuals' PHI: researcher
Article URL: http://www.databreaches.net/misconfigured-database-may-have-exposed-1-5-million-individuals-phi-researcher-2/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151222-05	Radiology Regional Centers	FL	12/22/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

The medical records, billing statements, registration information, and accounting records of hundreds of patients of Fort Myers-based Radiology Regional Centers have been found scattered in the street following an accident that occurred during their transportation from storage.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Hundreds of Medical Records Found Scattered in Street
Article URL: http://www.hipaajournal.com/hundreds-of-medical-records-found-scattered-in-street-8228/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151222-04	Hello Kitty	CA	12/21/2015	Electronic	Business	Yes - Unknown #	Unknown

The information exposed in the breach includes the first and last names, birth dates, genders, countries of origin, and email addresses for 3.3 million accounts.
It also includes lightly-protected passwords, as well as the forgotten password questions and answers. The passwords themselves are "hashed", a form of protection which renders it technically impossible to retrieve the original password. However, the hashing technique used by SanrioTown leaves it easy for an attacker to use force to uncover a significant proportion of the obscured passwords. The database was available online, where it was found by researcher Chris Vickery, who contacted security blog Salted Hash with the information over the weekend

Attribution 1 Publication: theguardian.com Author:
Article Title: Parents warned as Hello Kitty data breach leaks details of 3.3m user accounts
Article URL: http://www.theguardian.com/technology/2015/dec/21/hello-kitty-data-breach-leaks-details-3-3million-user-accounts

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151222-03	Thomas Nelson Community College	VA	12/18/2015	Electronic	Educational	Yes - Unknown #	Unknown

We learned on December 9, 2015, that on December 8, 2015, your confidential student information to include name, address, phone number, social security number, student identification number, date of birth, immunization dates, background check results (no offenses listed), grades, and student progress indicators were emailed to eleven current nursing students. Each of the email recipients has been contacted and directed to permanently delete this information.

Attribution 1 Publication: VT AG's office Author:
Article Title: Thomas Nelson Community College
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Thomas%20Nelson%20Community%20College%20SB

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151222-02	Dungarees	MO	12/18/2015	Electronic	Business	Yes - Unknown #	Unknown

We have recently learned that our online store was a victim of an illegal hack from a foreign entity, which may have resulted in a compromise to your credit card or debit card. On November 20, 2015, we first became aware of a possible breach when we discovered that our website had been manipulated by hackers. After this discovery, we took immediate action to secure our website, and we engaged a forensic IT firm to assist us in determining how this occurred.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151222-01	Department of Health	NM	12/15/2015	Electronic	Government/Military	Yes - Published #	561

A New Mexico Department of Health data breach report indicates 561 patients have had their Protected Health Information (PHI) exposed as a result of the theft of an unencrypted laptop computer from an employee's vehicle. An investigation was conducted to determine what data were stored on the laptop. Some of the information was password protected, although patient first and last names, dates of birth, medications, facility unit, and in some cases, medical diagnoses, were also stored on the laptop and could potentially be accessed by the thief.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: New Mexico Department of Health Data Breach Affects 561
Article URL: http://www.hipaajournal.com/new-mexico-department-of-health-data-breach-561-8233/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151221-05	Fox River Counseling Center / ST Psychotherapy, LLC	WI	12/21/2015	Electronic	Medical/Healthcare	Yes - Published #	509

Fox River Counseling Center, 627 Bay Shore Drive, is encouraging clients to change their passwords and monitor their accounts after someone stole an unsecured laptop Oct. 23, said Dr. Scott Trippe, a psychologist at the clinic. The computer contained outpatient mental health records of clients who visited the center from Nov. 7, 2012, to Aug. 19, 2014, and Wisconsin Disability Determination Bureau psychological evaluations from May 13, 2013, to Oct. 21, 2015. Information included in the data breach included clients' names, addresses, dates of birth, Social Security numbers, medical histories, mental status interviews, results of psychological testing, diagnoses and statements of work capacity, said Trippe, who himself had personal information on the laptop.

Attribution 1 Publication: databreaches.net / thenorthwestern.com Author:
Article Title: Mental health counseling clinic notifies patients after laptop with sensitive data stolen
Article URL: http://www.databreaches.net/wi-mental-health-counseling-clinic-notifies-patients-after-laptop-with-sensitive-data-stole

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151221-04	Landry's Inc.	TX	12/18/2015	Electronic	Business	Yes - Unknown #	Unknown

Landry's, Inc., which owns and operates several restaurant chains, yesterday announced that it had "received reports of unauthorized charges on certain payment cards after the cards were used legitimately at some of our restaurants."

Attribution 1 Publication: eSecurityPlanet.com Author: Jeff Goldman
Article Title: Landry's Restaurants Hit by Credit Card Breach
Article URL: http://www.esecurityplanet.com/network-security/landrys-restaurants-hit-by-credit-card-breach.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151221-03	VA New England Health System	MA	12/21/2015	Paper Data	Government/Military	Yes - Published #	259

One incident affected 259 veterans of the VA New England Health System in Boston, which resulted in their names, Social Security numbers, and procedure information being exposed. A clinic list was discovered in a public bathroom on November 5. The list had been printed on November 4, and according to the VA, it is unlikely that the list was dropped and left overnight. The restroom was maintained by housekeeping, which would have located the document had it been dropped the day previously. It is not clear how many individuals entered the bathroom and could potentially have viewed the information as the area was not covered by security cameras. Members of staff are to be re-informed on correct document handling procedures during the next staff meeting and credit monitoring services will be provided to all affected veterans.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: VA New England Health System
Article URL: http://www.hipaajournal.com/november-va-information-security-report-693-veterans-affected-in-november-2015-8226/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151221-02	Miami VA Healthcare System	FL	12/21/2015	Paper Data	Government/Military	Yes - Published #	126

The most serious privacy breach was reported by the Miami VA Healthcare System. The incident resulted in 126 veterans having their names, Social Security numbers, and IC-9 codes exposed. A nurse dropped two pages of a three-page report which was being used as part of a project to convert old IC-9 codes to the new IC-10 codes. The pages were dropped in a staff canteen and were not recovered. All affected veterans were offered credit monitoring services to mitigate risk.

Attribution 1
Publication: hipaajournal.com Author:
Article Title: Miami VA Healthcare System
Article URL: http://www.hipaajournal.com/november-va-information-security-report-693-veterans-affected-in-november-2015-8226/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151221-01	Office of Mary Ruth Buchness, MD, Dermatologist	NY	12/11/2015	Electronic	Medical/Healthcare	Yes - Published #	14,910

Specifically, on November 23, 2015, an email was sent to a number of current patients of our practice which was intended to include as an attachment a form of patient survey to help us improve our service to our patients. However, instead of the survey form, the email was inadvertently sent with an attachment that included a spreadsheet of demographic information regarding a number of our patients, which may have included you, containing names, social security numbers, dates of birth, gender, dates of last service and next appointment, telephone numbers, addresses, email addresses, marital status, head of household, employer/occupation and race/ethnicity.

Attribution 1
Publication: VT AG's office / hipaajournal.com Author:
Article Title: Office of Mary Ruth Buchness, MD, Dermatologist
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Buchness_%20MD%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151218-02	Corner Bakery	TX	12/21/2015	Electronic	Business	Yes - Unknown #	Unknown

What Happened? We value and respect the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved certain of your personal information. On November 10, 2015, we received a call from someone who alleged that an ex-employee of Corner Bakery possessed a file containing personal information of other company employees and expressed concern that the ex-employee may use that information for purposes of identity theft.

Attribution 1
Publication: CA AG's office Author:
Article Title: Corner Bakery
Article URL: https://oag.ca.gov/system/files/CBC_-_Sample_Notification_Letter_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151218-01	Camelback Women's Health	AZ	12/3/2015	Paper Data	Medical/Healthcare	Yes - Published #	810

Camelback Women's Health AZ Healthcare Provider 810 12/03/2015 Unauthorized Access/Disclosure Paper/Films

Attribution 1
Publication: hhs.gov Author:
Article Title: Camelback Women's 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
ITRC20151217-01	Safeway	CA	12/16/2015	Electronic	Business	Yes - Unknown #	Unknown

Sources at multiple financial institutions say they are tracking a pattern of fraud indicating that thieves have somehow compromised the credit card terminals at checkout lanes within multiple Safeway stores in California and Colorado. Safeway confirmed it is investigating skimming incidents at several stores.
Banking sources say they've been trying to figure out why so many customers in the Denver and Englewood areas of Colorado were seeing their debit cards drained of cash at ATMs after shopping at Safeways there. The sources compared notes and found that all of the affected customers had purchased goods from one of several specific lanes in different compromised stores (the transaction data includes a "terminal ID" which can be useful in determining which checkout lanes were compromised.

Attribution 1 Publication: KrebsonSecurity.com Author: Brian Krebs
Article Title: Skimmers Found at Some Calif., Colo. Safeways
Article URL: http://krebsonsecurity.com/2015/12/skimmers-found-at-some-calif-colo-safeways/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151216-01	Toyota Motor Credit Corporation	CA	9/15/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We are contacting you because we have become aware of a data security incident that involved some of your personal information. On August 5, 2015, an unencrypted email containing customer information was sent to a TFS vendor partner authorized to perform computer system enhancements. The email contained the following information associated with your account: name, TFS account number, bank account number and bank routing number.

Attribution 1 Publication: CA AG's office Author:
Article Title: Toyota Motor Credit Corporation
Article URL: https://oag.ca.gov/system/files/Vendor%20Partner%20Email%20Incident%20-%20Toyota%20States%20AG_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151215-09	Brenner McDonagh & Tortolani, Inc.	NY	11/30/2015	Electronic	Business	Yes - Unknown #	Unknown

On October 16, 2015, I3MT discovered that an employee unintentionally emailed a document containing personal information belonging to the nuns of one or its clients to two individuals at two other religious organizations. The document contained the sisters' name, address, date of birth, Social Security number, and limited health insurance information

Attribution 1 Publication: NH AG's office Author:
Article Title: Brenner McDonagh & Tortolani, Inc.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/brenner-mcdonagh-tortolani-20151130.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151215-08	New Dimension Group, LLC	NC	11/25/2015	Electronic	Medical/Healthcare	Yes - Published #	1,275

New Dimension Group, LLC NC Healthcare Provider 1275 11/25/2015 Loss Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: New Dimension 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
ITRC20151215-07	First Transit	OH	12/10/2015	Electronic	Business	Yes - Unknown #	Unknown

Malware inserted on a server on October 23, 2011 wasn't discovered until October 21, 2015, reports First Transit's external counsel. For almost four years, employees' information, including name, address, date of birth, phone number, driver's license number, and Social Security number may have been compromised.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: First Transit notifies employees after malware discovered on server
Article URL: http://www.databreaches.net/oh-first-transit-notifies-employees-after-malware-discovered-on-server/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151215-06	Office of Carolyn B. Lyde, MD, PA	TX	12/10/2015	Electronic	Medical/Healthcare	Yes - Published #	1,500

Carolyn B Lyde, MD, of Dermatology Center of Lewisville, Texas, notified HHS on November 30th that 1,500 patients were affected

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: 1,500 patients impacted by laptop theft
Article URL: http://www.databreaches.net/1500-patients-impacted-by-laptop-theft/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151215-05	Northwest Primary Care (NWPC)	OR	12/12/2015	Electronic	Medical/Healthcare	Yes - Published #	5,372

A former employee of Portland-based Northwest Primary Care (NWPC) stole the Protected Health Information (PHI) of 5,372 patients of the Oregon medical clinic, according to a NWPC breach notice issued yesterday

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Former Northwest Primary Care Employee Stole 5,372 Patient Records
Article URL: http://www.hipaajournal.com/former-northwest-primary-care-employee-stole-5372-patient-records-8214/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151215-04	California Virtual Academies (CAVA)	CA	12/12/2015	Electronic	Educational	Yes - Unknown #	Unknown

California Virtual Academies (CAVA) is a network of 11 publicly funded charter k-12 schools in California. Researcher Chris Vickery recently contacted DataBreaches.net after he found a database with 58,694 of their students' records leaking. In addition to a lot of personal information on the students that was all in plain text, the leaking data included some information on student disabilities and special education needs, services, and goals – again, all in plain text.

Attribution 1 Publication: databreaches.net Author:
Article Title: Personal and sensitive data of 59,000 charter school students in California leaked: researcher
Article URL: http://www.databreaches.net/personal-and-sensitive-data-of-59000-charter-school-students-in-california-leaked-resear

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151215-03	TuneCore	NY	11/23/2015	Electronic	Business	Yes - Unknown #	Unknown

TuneCore recently discovered suspicious activity on its servers, including the illegal collection of certain personal and account information. This information may have included your Social Security or taxpayer ID number and date of birth, as well as your royalty statements for the third quarter of 2015, showing the number of sales or downloads on different platforms, along with the contractual rate for them, and the sum of transactions. It may also have included your name, address, email address, TuneCore account number, and protected TuneCore password. In addition, if you provided us with billing information, the information illegally accessed may have included your billing address; the last 4 digits of your credit card number, as well as its expiration date; your bank name and the last 4 digits of your bank account number and the last 4 digits of your bank routing number; and the name and address associated with the bank account. TuneCore does not store any full financial account information.

Attribution 1 Publication: CA AG's office / VT AG's office Author:
Article Title: TuneCore
Article URL: https://oag.ca.gov/system/files/TuneCore_Customer_Letter_Template_SSN_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151215-02	Sorrento Pacific Financial, LLC	CA	12/14/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Breach notification letter unavailable on CA AG site.

Attribution 1 Publication: CA AG's office Author:
Article Title: Sorrento Pacific Financial, LLC
Article URL: https://oag.ca.gov/ecrime/databreach/reports/sb24-59275

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151215-01	MacKeeper	CA	12/15/2015	Electronic	Business	Yes - Unknown #	Unknown

An information security researcher warns that he was able to find online "sensitive account details" relating to a heavily marketed - and controversial - application called MacKeeper. "I have recently downloaded over 13 million sensitive account details related to MacKeeper, Zeobit, and/or Kromtech [Alliance]," Texas-based information security researcher Chris Vickery says in a Dec. 14 post to news website Reddit, referring respectively to MacKeeper's previous and current owners.

Attribution 1 Publication: DataBreachtoday.com Author: Mathew J. Schwartz
Article Title: MacKeeper: 13M Customers' Details Exposed
Article URL: http://www.databreachtoday.com/mackeeper-13m-customers-details-exposed-a-8749?rf=2015-12-15-edbt&mkt_tok=3R

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151214-06	**PeaceHealth St. John Medical Center**	WA	12/10/2015	Electronic	Medical/Healthcare	Yes - Published #	**1,407**

Two cases of PHI theft by employees have been discovered in Washington Medical facilities run by PeaceHealth. The first occurred in August, 2015 and affected patients of the PeaceHealth Southwest Medical Center, WA. The second occurred in October and affected patients of the PeaceHealth St. John Medical Center, WA. According to a breach notice placed on the healthcare provider's website, the first breach affected 346 patients and the second affected 595 patients.

The first data breach involved an employee emailing data to a personal account from the hospital, while the second was caused when an employee accessed the healthcare provider's system via third party websites after leaving employment.

According to the OCR breach reporting portal a PeaceHealth data breach was been added yesterday that indicates 1,407 patients have been impacted. It would appear that the second data breach is more serious than initially thought.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Two Cases of Healthcare Employee Data Theft Uncovered by PeaceHealth
Article URL: http://www.hipaajournal.com/5-cases-healthcare-employee-data-theft-8211/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151214-05	**PeaceHealth Southwest Medical Center**	WA	12/10/2015	Electronic	Government/Military	Yes - Published #	**346**

The first occurred in August, 2015 and affected patients of the PeaceHealth Southwest Medical Center, WA. The second occurred in October and affected patients of the PeaceHealth St. John Medical Center, WA. According to a breach notice placed on the healthcare provider's website, the first breach affected 346 patients and the second affected 595 patients. The first data breach involved an employee emailing data to a personal account from the hospital, while the second was caused when an employee accessed the healthcare provider's system via third party websites after leaving employment.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Two Cases of Healthcare Employee Data Theft Uncovered by PeaceHealth
Article URL: http://www.hipaajournal.com/5-cases-healthcare-employee-data-theft-8211/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151214-04	**Community Mercy Health Partners**	OH	12/11/2015	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

On Thanksgiving day, Leroy Clouser of Springfield, Ohio, says he made a stunning discovery while dropping off some items at an area recycling center: Dumpsters contained patient medical records and other paperwork and folders displaying the names of Community Mercy Health Partners and some of its current and former facilities, including Mercy Memorial Hospital, Community Hospital and Springfield Regional Medical Center.

Attribution 1 Publication: healthcareinfosecurity.com Author: Marianne Kolbasuk M
Article Title: Paper Records Disposal Still a Messy Problem
Article URL: http://www.healthcareinfosecurity.com/paper-records-disposal-still-messy-problem-a-8744?rf=2015-12-14-eh&mkt_tok

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151214-03	**Woodland Heights Medical Center**	TX	12/10/2015	Paper Data	Medical/Healthcare	Yes - Published #	**450**

A Texas ranger recently discovered that a former employee of Woodland Heights Medical Center in Lufkin, TX, had been stealing patient medical records while employed at the hospital. A search of the employee's home revealed approximately 450 "face sheets" had been taken from the hospital.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Woodland Heights Medical Center Employee Stole 450 Patient Records
Article URL: http://www.hipaajournal.com/5-cases-healthcare-employee-data-theft-8211/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151214-02	Middlesex Hospital	CT	12/9/2015	Electronic	Medical/Healthcare	Yes - Published #	946

What happened? In October four hospital employees were victimized by a phishing campaign. What type of information? The information involved includes the patients name, address, date of birth, medical record number, medication, date of service and the date of diagnosis. The compromised information did not include Social Security numbers or any access to a person's full medical records.

Attribution 1 Publication: Scmagazaine.com / hhs.gov Author: Doug Olenick
Article Title: Phishing scam hits Middlesex Hospital in Conn.
Article URL: http://www.scmagazine.com/phishing-scam-hits-middlesex-hospital-in-conn/article/458813/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151214-01	New England Calendar and Novelty Company	NY	12/9/2015	Electronic	Business	Yes - Unknown #	Unknown

We have learned that, due to a security breach involving our website (http:f/www.newenglandcalendar.com), an unauthorized and unknown party was able to access the information of customers that had purchased products online from New England Calendar. We have determined that your personal information, such as your name, address, e-mail address, site password, and payment card information, was accessed on or around September 24, 2015 and may have been compromised.

Attribution 1 Publication: VT AG's office Author:
Article Title: New England Calendar and Novelty Company
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/NE%20Calendar%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151210-01	Elephant Bar / CM Bar	TX	12/9/2015	Electronic	Business	Yes - Unknown #	Unknown

The owner of the Elephant Bar restaurant chain says a potential data breach could affect customers in seven states who paid with credit or debit cards. CM Ebar says the security incident involves nearly 30 Elephant Bar locations, eight of them in the San Francisco Bay Area. The Dallas-based chain on Tuesday apologized for the apparent breach and urged customers to review their card statements. Elephant Bar on Nov. 3 was alerted by its card processor about illegal software found on payment processing systems in certain restaurants.

Attribution 1 Publication: San Jose Mercury News Author:
Article Title: Elephant Bar data breach includes 8 Bay Area sites since August
Article URL: http://www.mercurynews.com/business/ci_29223702/elephant-bar-data-breach-includes-8-bay-area

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151209-02	Citizens Financial Group, Inc.	RI	12/2/2015	Paper Data	Banking/Credit/Financial	Yes - Published #	498

On November 9, 2015, a customer complaint was received indicating that a customer was mailed their monthly escrow statement and the mailing contained two other customer escrow statements. The escrow statement contained customer name, address, and account number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Citizens Financial Group, Inc.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/citizens-20151202.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151209-01	Ameriprise Financial, Inc.	MN	11/25/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

I am writing to make you aware of an incident involving your personal information. On October 13, 2015, I had problems with my computer and allowed a third party to connect to my computer to fix the issue. The connection allowed access to the files on my computer. Unfortunately, business files on my computer contained your name, address, date of birth, Social Security and account numbers. There is no evidence to indicate that your information was accessed by the third party, however, I wanted to take the precaution of notifying you.

Attribution 1 Publication: NH AG's office Author:
Article Title: Ameriprise Financial, Inc.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/ameriprise-financial-20151125.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151208-07	Cigna Home Delivery	CT	11/23/2015	Paper Data	Medical/Healthcare	Yes - Published #	592

Cigna Home Delivery Pharmacy CT Healthcare Provider 592 11/23/2015 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Cigna Home Delivery
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
ITRC20151208-06	Alaska Orthopedic Specialists, Inc.	AK	11/19/2015	Electronic	Medical/Healthcare	Yes - Published #	553

Alaska Orthopedic Specialists, Inc. AK Healthcare Provider 553 11/19/2015 Theft Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Alaska Orthopedic Specialists, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=144FDE00942551A30F110860E76D3A62.ajp13w

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151208-05	WakeMed	NC	12/4/2015	Electronic	Medical/Healthcare	Yes - Published #	158

A Cary law firm has filed a motion against WakeMed, accusing the hospital of releasing patients' private information, including Social Security numbers, making them susceptible to identity theft.

Attribution 1 Publication: WRAL.com / databreaches.net Author:
Article Title: Attorney: WakeMed violated patients' privacy, released sensitive information
Article URL: http://www.wral.com/attorney-wakemed-violated-patients-privacy-released-sensitive-information/15154432/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151208-04	Hellgate High / Missoula County Public School District	MT	12/8/2015	Electronic	Educational	Yes - Unknown #	Unknown

Missoula County Public School District one is investigating why a bunch of private, confidential information about Hellgate students and one school staffer were sent to parents of Hellgate High School football players last Friday. The information included very sensitive details, including which students at school were failing classes, which students were seeking mental health counseling and even details about family-abuse cases.

Attribution 1 Publication: newstalkkgvo.com Author:
Article Title: Hellgate High Data Breach Reveals Confidential Student Information
Article URL: http://newstalkkgvo.com/hellgate-high-data-breach-reveals-confidential-student-information/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151208-03	MaineGeneral Health and its subsideraries	ME	12/8/2015	Electronic	Medical/Healthcare	Yes - Published #	500

On November 13, 2015, MaineGeneral was notified by the Federal Bureau of Investigation (FBI) of the detection of certain MaineGeneral data on an external website, which is not accessible by the general public. MaineGeneral immediately hired a highly respected cyber security forensics firm and launched an internal investigation by its IT team to confirm the security of our system and source of the data breach, and continues to cooperate with the FBI.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: MaineGeneral Health notifying employees and patients after FBI alerts them to breach
Article URL: http://www.databreaches.net/mainegeneral-health-notifying-employees-and-patients-after-fbi-alerts-them-to-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151208-02	Blue Cross Blue Shield Nebraska	NE	12/3/2015	Electronic	Medical/Healthcare	Yes - Published #	1,872

The error resulted in Explanation of Benefits (EoB) statements being sent to the wrong customers, and divulged patients names, ID numbers, and dental claim information, including the services that had been covered by members' health insurance policies. The unauthorized disclosure affected 1,872 BCBS members.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Another HIPAA Breach Courtesy of a Printing Error
Article URL: http://www.hipaajournal.com/another-hipaa-breach-courtesy-of-a-printing-error-8205/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151208-01	University of Colorado Health	CO	12/7/2015	Electronic	Medical/Healthcare	Yes - Published #	827

Aurora-based University of Colorado Health began notifying more than 800 patients Thursday that an employee inappropriately gained access to their health records out of "personal curiosity," according to a news release.

Attribution 1 Publication: Beckershospitalreview.com / hhs.gov Author:
Article Title: UCHealth fires employee who inappropriately accessed more than 800 patient records
Article URL: http://www.beckershospitalreview.com/healthcare-information-technology/uchealth-fires-employee-who-inappropriate

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151207-05	Kalahari Resorts	WI	12/7/2015	Electronic	Business	Yes - Unknown #	Unknown

In late October, officials were alerted that an intruder installed malware designed to capture data from certain payment cards from a limited number resort outlets including restaurants, bars, retail and spa, between May 18, 2015 and Nov. 9, 2015. The attacker didn't access the front desk POS system.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Kalahari Resorts hit by POS breach
Article URL: http://www.scmagazine.com/second-wisconsin-dells-based-resort-hit-by-breach/article/458238/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151207-04	MUJI USA, LIMITED	NJ	11/16/2015	Electronic	Business	Yes - Unknown #	Unknown

Unfortunately, like many companies in today's global online economy, we received information suggesting that we may have experienced a data compromise. Immediately, we closed our online web shop in order to protect our customers. We regret that we might have caused any inconvenience for you due to the closure of our online shopping site.

Attribution 1 Publication: CA AG's office Author:
Article Title: MUJI USA, LIMITED
Article URL: https://oag.ca.gov/system/files/Muji%20USA%20notice%20only_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151207-03	Centegra Health System	IL	12/3/2015	Paper Data	Medical/Healthcare	Yes - Published #	2,929

The data breach was caused as a result of a simple error made by an employee of MedAssets. The company had been contracted to mail billing statements to patients. An error was made configuring the equipment used to prepare the mailing, which resulted in patients being sent two billing statements instead of one. One of the statements was correct and included patients' personal data and charges, the other statement was for a different patient. Each envelope was filled automatically and was mailed. 2,929 letters were sent to patients by MedAssets between November 2 and Nov 6, 2015.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: CENTEGRA DATA BREACH EXPOSES PHI OF 3,000 PATIENTS
Article URL: http://www.hipaajournal.com/centegra-data-breach-3000-patients-8198/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151207-02	Santa Barbara Department of Health	CA	12/3/2015	Electronic	Medical/Healthcare	Yes - Published #	260

The HIPAA privacy rule violation occurred when an employee accessed Protected Health Information of 260 individuals as part of a research project, but had not obtained prior authorization to access the data. Consequently, the employee breached the HIPAA Privacy Rule. The research project had not been authorized by the Public Health Dept., and the accessing of patient data was therefore illegal.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: SANTA BARBARA PUBLIC HEALTH DEPT. ANNOUNCES HIPAA PRIVACY RULE VIOLATION
Article URL: http://www.hipaajournal.com/santa-barbara-public-health-dept-hipaa-privacy-rule-violation-8200/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151207-01	Springfield Community Hospital	OH	12/6/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Medical records from a now defunct Ohio hospital have recently been discovered in a public dumpster. Hundreds of confidential medical records containing highly sensitive medical and personal information were found at a recycling center by a member of the public. The documents contained patient names, dates of birth, Social Security numbers, and medical test results, some of which could potentially be used to discriminate against individuals. According to a recent report on WDTN news, the medical data contained in the documents included STD test orders, gynecological examination reports, and drug screening test results. The records related to patients who had received treatment in 2005 and 2006, although some older records were also discovered.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: SPRINGFIELD COMMUNITY HOSPITAL MEDICAL DATA DISCOVERED IN DUMPSTER
Article URL: http://www.hipaajournal.com/springfield-community-hospital-medical-data-discovered-in-dumpster-8203/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151204-04	Knit-Rite, Inc.	KS	12/1/2015	Electronic	Business	Yes - Unknown #	Unknown

On October 27, 2015, we were alerted to a potential security incident involving the Websites. Based upon an extensive forensic investigation, it appears that unauthorized individuals installed malicious software on the servers hosting the Websites that was designed to capture user account and payment card information as it is inputted into those systems. We believe that the malware could have compromised certain information (including name, address, website username and password, e-mail address, payment card account number, card expiration date, and payment card security code) of individuals who made a purchase on the Websites between February 17, 2015, and May 27, 2015.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151204-03	Cottage Health	CA	12/2/2015	Electronic	Medical/Healthcare	Yes - Published #	11,000

Cottage Health's efforts to protect the confidentiality of hospital patient records suffered a setback earlier this fall when one of its computer servers was found to be exposed to possible outside access. In a statement released Wednesday afternoon, Cottage Health officials said limited information from as many as 11,000 patients was exposed.

Attribution 1 Publication: noozhawk.com / CA AG's office / hhs.go Author:
Article Title: Cottage Health Notifying Patients of Potential Records Breach
Article URL: http://www.noozhawk.com/article/cottage_health_notifying_patients_of_potential_information_breach_20151202

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151204-02	Keenan & Associates	CA	10/9/2015	Electronic	Business	Yes - Published #	35,000

On October 9, 2015, we learned that documents containing information relating to some employees and some of their dependents could potentially be found through searches on the Internet. We immediately began an investigation and discovered that the documents may have been made available on the Internet when a vendor misconfigured security settings on the portal where the documents were stored. The portal settings have since been reconfigured and the documents are no longer searchable on the Internet.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: CALIFORNIAN HEALTH PLAN ADMINISTRATOR ANNOUNCES 35K-RECORD DATA BREACH
Article URL: http://www.hipaajournal.com/californian-health-plan-administrator-35k-record-data-breach-8201/

Attribution 2 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Keenan & Associates
Article URL: https://oag.ca.gov/system/files/Keenan%20Associates%20Ad%20r3fin_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151204-01	**Office of Holly A. Nordhues, CPA**	CA	11/24/2015	Electronic	Business	Yes - Unknown #	**Unknown**
	Notification letter unavailable						

Attribution 1 Publication: CA AG's office Author:
Article Title: Office of Holly A. Nordhues, CPA
Article URL: https://oag.ca.gov/ecrime/databreach/reports/sb24-59137

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-18	**Honey Baked Ham Company, LLC / Stoner Bunting**	PA	10/26/2015	Electronic	Business	Yes - Unknown #	**Unknown**
	On October 15, 2015, SBA became aware of suspicious activity occurring on its website. Upon initial investigation, SBA realized that malware had been installed in the website software by an unauthorized source which “listened” to the website visitor’s information and appears to have been able to capture such information. Consequently, the hacker had access to the personal information of the individuals, which included first and last names, addresses and credit card information. SBA is currently unaware of any actual unauthorized access to or transmission of personal information from SBA’s website.						

Attribution 1 Publication: MD AG's office Author:
Article Title: Stoner Bunting Advertising
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260737.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-17	**Stonebridge Life**	TX	10/12/2015	Electronic	Business	Yes - Unknown #	**Unknown**
	One of our employees sent a completed Beneficiary form that included personally identifiable information that included date of birth and Social Security number on October 6, 2015. This breach was reported on October 7, 2015 and reported in an incident report to our security team the same day and began our internal investigation Information included names, addresses, social security numbers, dates of birth, policy number.						

Attribution 1 Publication: MD AG's office Author:
Article Title: Stonebridge Life
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260730.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-16	**Office of Peggy Olson**	ND	10/9/2015	Electronic	Business	Yes - Unknown #	**Unknown**
	On September 2, 2015, a virus infected my computer and an unauthorized indMdual may have gained access to my computer for a limited period of time -less than one hour. While your information was stored in a file on my computer and I think it highly unlikely that the unauthorized individual accessed your information, I wanted to let you know about this event out of an abundance of caution. The file may have contained your name, address, and Social Security number.						

Attribution 1 Publication: MD AG's office Author:
Article Title: Office of Peggy Olson
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260725.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-15	Integrated Listening Systems	CO	10/22/2015	Electronic	Business	Yes - Unknown #	Unknown

We recently discovered malicious code on our e-commerce website. We believe that the malicious code was inserted on May 18, 2015 through a breach in the site.
The malicious code appears to have allowed hackers to capture data entered in the checkout page by users of the website.

Attribution 1 Publication: MD AG's office Author:
Article Title: Integrated Listening Systems
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-259986.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-14	Teach for America	NY	9/30/2015	Electronic	Business	Yes - Unknown #	Unknown

On July 29, 2015, property was stolen out of a secured vehicle used by a Teach for America employee. The stolen property included paper files, a USB drive, and a password-protected laptop computer owned by Teach for America and used by the employee to perform work duties. Through this investigation, Teach for America determined the laptop, USB drive and paper files may have contained the name, Social Security number, and financial information such as bank account number, for certain individuals at the time of the theft. These individuals were current and former affiliates of Teach for America or Teach for America-sponsored initiatives.

Attribution 1 Publication: MD AG's office Author:
Article Title: Teach for America
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260693.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-13	Lando Law Firm	SC	9/1/2015	Electronic	Business	Yes - Unknown #	Unknown

On or about J u.ne 3, 2015, the firm became the victim of a targeted phishing attack. As a result, the attackers obtained access to a firm email account intermittently on June 3 through June 4, 2015. We are writing to inform you that, through our ongoing investigation, we have learned that some of your personal information, including Social Security Number, bank account number, and driver's license number, may have been accessible during the attack.

Attribution 1 Publication: MD AG's office Author:
Article Title: Lando Law Firm
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257998.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-12	TD Bank	NJ	8/18/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently experienced a privacy issue but we're making things right. We recently learned that one of our employees may have improperly obtained some of your personal information. The personal information potentially exposed may have included your name, address and account number.

Attribution 1 Publication: MD AG's office Author:
Article Title: TD Bank
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257982.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-11	Columbia Eye Care	MD	8/19/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

We are writing to inform you that there possibly may have been a security breach with your credit card number on August 5, 2015. During the office renovation, our safe was stolen along with its contents which included the daily paperwork. There were no credit card expiration dates, three digit security codes or personal information in the contents of the safe. There is a police report filed with Howard County Police.

Attribution 1 Publication: MD AG's office Author:
Article Title: Columbia Eye Care
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257966.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-10	Mountain Travel Sobek	CA	10/29/2015	Electronic	Business	Yes - Unknown #	Unknown

Immediately upon discovering the theft of the laptop,we launched an internal investigation to determine what information might have been stored on the laptop at the time of the theft. While our investigation is ongoing, we determined on October 2, 2015 that the stolen laptop contained certain information about you, including your name, address and Social Security number. We are unaware of any actual or attempted misuse of your information, and there is no indication that the information stored on the laptop was the target of the theft.

Attribution 1 Publication: MD AG's office Author:
Article Title: Mountain Travel Sobek
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260740.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-09	Red Dress Boutique	GA	10/6/2015	Electronic	Business	Yes - Published #	295

On September 15, we discovered that some foreign code was inserted and/or activated on the site at 5:40am ET on September 14. We do not store credit card data; nor do we have any access to it. So no historical credit card information was at risk. However, we cannot eliminate the possibility that credit card information could have been intercepted for transactions during that roughly 30-hour period.

Attribution 1 Publication: MD AG's office Author:
Article Title: Red Dress Boutique
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260754.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-08	UC Health, LLC	OH	11/14/2015	Electronic	Medical/Healthcare	Yes - Published #	1,064

UC Health issued a statement late last week saying, it is "notifying 1,064 patients regarding a privacy incident involving some of their patient information." UC Health spokeswoman Diana Lara says it appears social security numbers may have been included in some of the outgoing email messages, but Lara says it appears the number of emails with that kind of sensitive data numbers around 10.

Attribution 1 Publication: hhs.gov / WLWT.com Author:
Article Title: UC Health investigating possible data breach
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-07	Midlands Orthopaedics, P.A.	SC	11/13/2015	Electronic	Medical/Healthcare	Yes - Published #	3,902

Midlands Orthopaedics, P.A. SC Healthcare Provider 3902 11/13/2015 Hacking/IT Incident Network Server

Business Associate Present: Yes

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-06	Spring Mountain Capital / KPMG	NY	10/1/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently learned that, on September 12, 2015, due to a technical glitch, KPMG LLP ("KPMG"), who is the independent auditor of SMC Reserve Fund II, LP (the "Fund"), inadvertently sent certain flies containing draft tax forms to the online file sharing account of an unintended third-party user. The forms contained certain personal information, including names, addresses and Social Security numbers, of some Fund investors.

Attribution 1 Publication: MD AG's office Author:
Article Title: Spring Mountain Capital / KPMG
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260724.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-05	John Carroll University	OH	10/5/2015	Electronic	Educational	Yes - Unknown #	Unknown

Following external and internal webserver scans, JCU's Information Technology Services team ("ITS") learned on July 30, 2015 that one of its web servers had been compromised with malware which allowed potential unauthorized access to personally identifiable information. JCU determined that the server contained personal information that may have been subject to unauthorized access, including a combination of their names, dates of birth, Social Security numbers, and addresses. We are unaware of any actual access to this specific information or any misuse of this information by unauthorized persons.

Attribution 1 Publication: MD AG's office Author:
Article Title: John Carroll University
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260711.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-04	Quad/Graphics	WI	8/13/2015	Electronic	Business	Yes - Published #	693

More specifically, on July 20, 2015, we intended to send an informational email to a group of Quad employees impacted by a change in our Pay Card process. In the course of doing so, we unintentionally sent the message with an attached spreadsheet containing certain personal information for the employees receiving the email

Attribution 1 Publication: MD AG's office Author:
Article Title: Quad/Graphics
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257991.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-03	Northwest Georgia Housing Authority	GA	10/5/2015	Paper Data	Business	Yes - Unknown #	Unknown

On September 11 , 2015, we learned that certain private or personal information may have been publicly displayed and/or published without authorization by a former Northwest Georgia Housing Authority employee. Subsequently, we determined that some of your personal identifying information was likely disclosed/posted to a public bulletin board located at some of our housing offices.
As a result of this incident, other persons or individuals may have obtained some of your personal identifying information, including your name, home address, phone number, date of birth, and Social Security number. We have no reason to believe at this time that your information will be used in an inappropriate way.

Attribution 1 Publication: MD AG's office Author:
Article Title: Northwest Georgia Housing Authority
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260710.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-02	Smartlabtoys.com	WA	9/28/2015	Electronic	Business	Yes - Unknown #	Unknown

Pursuant to Maryland Code, we are writing to notify you that on July 16, 2015 we uncovered evidence of a sophisticated cyber attack perpetrated against our website. Www.smartlabtoys.com that may have resulted in a data breach of some of our customers' personal information. Along with our customers' names, shipping and billing address(es), email address, and telephone number, it is possible that their credit card information was compromised. Five of our customers who information may have been compromised have a billing address located in Maryland state.

Attribution 1 Publication: MD AG's office Author:
Article Title: Smartlabtoys.com
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260691.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151201-01	Vmware, Inc.	CA	8/19/2015	Electronic	Business	Yes - Unknown #	Unknown

On July 2, 2015, we determined that there has been unauthorized access to some VMware email accounts and consequently there may have been unauthorized access to the messages stored in those accounts, including their attachments. We regret that this incident occurred and take the security of personal information very seriously. We have determined that the personal information involved in this incident included your name and may have included driver's license, credit card information, and financial account numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Vmware, Inc.
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257989.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151130-09	Gallagher Bassett Services	IL	8/13/2015	Electronic	Business	Yes - Unknown #	Unknown

On July 27, 2015, Gallagher Bassett Services, Inc. learned that a member of our claims adjustment team was a victim of theft of her laptop computer resulting from the break-in of her automobile on July 24, 2015. Gallagher Bassett immediately started its investigation to determine what information may be at risk as a result of the theft. We discovered that the hard drive of the laptop computer and paper files may have contained some personal information, including name, address, social security number, driver's license, and/or some claim and claim-related health information, of the affected resident that was reviewed by the claims adjuster while processing the affected resident's

Attribution 1 Publication: MD AG's office Author:
Article Title: Gallagher Bassett Services
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257958.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151130-08	Nationwide	OH	8/13/2015	Electronic	Business	Yes - Unknown #	Unknown

On July 29, 2015, we discovered that we had inadvertently included two of your employer's documents in an email to a different Retirement Plan client. The documents contained your Name, Social Security Number, Date of Birth and Hire Date. We have identified the cause of the mistake and have taken appropriate steps to address the error.

Attribution 1 Publication: MD AG's office Author:
Article Title: Nationwide
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257955.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151130-07	SMS Hospitality	MD	8/5/2015	Electronic	Business	Yes - Unknown #	Unknown

On June 29, 2015, we discovered that an employee had connected a small data capture device to the back of the guest registration computer at the front desk of the Hotel. We initiated an investigation and immediately contacted the Orlando police department. We provided the identity of the employee to the Orlando police department, and that person is no longer employed by us. If so, the device could have recorded information from payment cards used at that register from approximately May 28, 2015 (the first day the employee started working without a trainer) until June 29, 2015 (when the device was removed). This information may have included the cardholder's name, card number, expiration date, verification code, and email address.

Attribution 1 Publication: MD AG's office Author:
Article Title: SMS Hospitality
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257938.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151130-06	Principal Financial Group	IA	8/3/2015	Paper Data	Banking/Credit/Financial	Yes - Unknown #	Unknown

The purpose for our letter is to notify you that your personal information was included on a retirement benefit quote, which was inadvertently mailed to an incorrect address. The retirement benefit quote included your personal information, including your Name, Social Security Number and Date of Birth.

Attribution 1 Publication: MD AG's office Author:
Article Title: Principal Financial Group
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257937%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151130-05	Oiselle.com	OR	11/24/2015	Electronic	Business	Yes - Unknown #	Unknown

Regretfully, on Thursday. November, 5, 2015, we learned that Oiselle.com was the target of criminal hackng activity, resulting in the theft of some of our customer transaction data for transactions that occurred between October 29, 2015 and November 5, 2015. In reviewing our records, we have determined that your information may have been affected. Specifically, based on our investigation the attacker obtained access to your name, email address, billing address, credit card number, expiration month and year, and three-digit security code used for the order placed during that time frame.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151130-04	DeKalb County School System	GA	11/27/2015	Electronic	Educational	Yes - Unknown #	Unknown

Just one day after that massive data leak from the Georgia Secretary of State's office there was yet another one. This one involved hundreds of teachers from the DeKalb County School System. The breach was part of a mass email that was sent out to the system's special education teachers. But somehow, sensitive information was attached and exposed. The emails were later deleted but not before being seen by an undetermined number of people.

Attribution 1 Publication: 11alive.com / databreaches.net Author:
Article Title: Hundreds of DeKalb teachers' personal information exposed
Article URL: http://www.11alive.com/story/news/education/2015/11/20/dekalb-county-teachers-personal-information-exposed/76146

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151130-03	Amazon Password Breach	WA	11/25/2015	Electronic	Business	Yes - Unknown #	Unknown

Online retailer Amazon on Tuesday started sending emails to some of its users, prompting them to reset their passwords, saying that they might have been compromised. The company informed users that it decided to force-reset their passwords after learning that they might have been exposed to a third party. The emails sent out by Amazon also suggested that the company adopted this precautionary measure although it was not aware of user passwords being improperly disclosed, ZDNet reports.

Attribution 1 Publication: securityweek.com Author:
Article Title: Amazon Forces Password Resets after Possible Security Breach
Article URL: http://www.securityweek.com/amazon-forces-password-resets-after-possible-security-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151130-02	Pathways Professional Counseling	AL	11/28/2015	Electronic	Medical/Healthcare	Yes - Published #	986

A breach of social security numbers, health insurance information, medical data, and personally identifiable information has been announced by Pathways Professional Counseling after a laptop computer was stolen from the vehicle of an employee. The laptop computer was password protected, but was not encrypted. The device contained highly sensitive information that could potentially be used by criminals to commit identity theft and fraud. Other data stored on the laptop included patient names, dates of birth, addresses, email addresses, phone numbers, demographic data, clinical information, financial information, referring physician names, and medical diagnoses of patients.

Attribution 1 Publication: hipaajournal.com / healthitsecurity.com Author:
Article Title: PATHWAYS PROFESSIONAL COUNSELING REPORTS THEFT OF LAPTOP CONTAINING SSNS
Article URL: http://www.hipaajournal.com/pathways-professional-counseling-reports-theft-of-laptop-containing-ssns-8193/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151130-01	Vtech	OR	11/30/2015	Electronic	Business	Yes - Unknown #	Unknown

VTech, the maker of tablets and gadgets aimed at children, confirmed 5 million accounts were impacted by a breach of an app store database uncovered by the company earlier this month. In a statement released Monday, VTech says the database contained profile information including names, email addresses, download history, passwords and mailing addresses. The database also included information on kids including names, genders and birthdates. VTech notes the database did not store credit card information or personal identification data such as social security numbers.

Attribution 1 Publication: usatoday.com / CA AG's office Author:
Article Title: VTech data breach impacts 5 million accounts
Article URL: http://www.usatoday.com/story/tech/2015/11/30/vtech-data-breach-impacts-5-million-accounts/76562538/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151125-01	LANDESK	UT	11/25/2015	Electronic	Business	Yes - Unknown #	Unknown

On Nov. 18, 2015, LANDESK sent a letter to current and former employees warning of an intrusion, stating that “it is possible that, through this compromise, hackers obtained personal information, including names and Social Security numbers, of some LANDESK employees and former Wavelink employees.”

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Breach at IT Automation Firm LANDESK
Article URL: http://krebsonsecurity.com/2015/11/breach-at-it-automation-firm-landesk/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-21	Wilderness Resort	WI	11/23/2015	Electronic	Business	Yes - Unknown #	Unknown

Guests who used their debit or credit card to pay for or place hotel reservations or to make purchases at onsite food and beverage outlets, attractions and retail locations between March 9, 2015 and June 8, 2015 could potentially be affected. The resort’s system to process online gift card purchases or the computer system used to process purchases at off-site food and beverage locations, including Field’s at the Wilderness, Sarento’s and Monk’s or Sundara Spa, were not affected.

Attribution 1 Publication: channel3000.com Author:
Article Title: Data breach affects Wilderness Resort visitors
Article URL: http://www.channel3000.com/money/data-breach-affects-wilderness-resort-visitors/36611576

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-20	Office of Dr. Mary Ruth Buchness	NY	11/24/2015	Electronic	Medical/Healthcare	Yes - Published #	15,000

When Missy Brown opened her email Monday morning, she was stunned to find a document from her doctor's office containing personal information for 15,000 names. "I think the subject line said 'coupon attached,' and I saw that there was a spreadsheet attachment," she said. "As soon as I opened it, I saw that it was a spreadsheet that had personal information in it." The document was a detailed list of nearly 15,000 names and corresponding addresses, appointment dates and Social Security numbers, all from the office of Dr. Mary Ruth Buchness, a dermatologist in Soho. It's not clear how and why the file was sent out.

Attribution 1 Publication: databreaches.net / News4NewYork Author:
Article Title: NYC Doctor's Office Emails Spreadsheet Containing Personal Info for 15K Patients
Article URL: http://www.nbcnewyork.com/news/local/New-York-City-Doctor-Emails-Personal-Information-Spreadsheet-Patients-353

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-19	Alliance Health Management & Consulting Inc.	TX	11/24/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

A defunct home health care management company that was based in San Antonio has been sued by the state over clients’ personal information found in a recycling container at Stevenson Middle School. Files belonging to Alliance Health Management & Consulting Inc. were recovered by Northside Independent School District police officers on July 14, 2014, and eventually were turned over to the Texas attorney general’s office, according to a lawsuit filed against the company.

Attribution 1 Publication: databreaches.net Author:
Article Title: State sues defunct health care management firm after health records found in recycling bin
Article URL: http://www.databreaches.net/tx-state-sues-defunct-health-care-management-firm-after-health-records-found-in-recycli

Attribution 2 Publication: hipaajournal.com Author:
Article Title: TEXAS ATTORNEY GENERAL TAKES ACTION OVER IMPROPER DISPOSAL OF PHI
Article URL: http://www.hipaajournal.com/texas-attorney-general-takes-action-over-improper-disposal-of-phi-8190/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-18	Jefferson County	CO	11/24/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

As public anxiety persists over regular reports of major data breaches, Social Security numbers of up to thousands of current and former Jefferson County residents can be found online in electronic county records, increasing locals' vulnerability to a costly and stressful ordeal.

Attribution 1 Publication: databreaches.net / beaumont enterprise Author:
Article Title: Personal data of thousands of Jefferson Co. residents exists online
Article URL: http://www.beaumontenterprise.com/news/article/Personal-data-of-thousands-of-Jefferson-Co-6651785.php

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-17	Kohl's	WI	9/29/2015	Electronic	Business	Yes - Unknown #	Unknown

We recently learned of an incident involving the compromise of some personal information of certain Kohl's customers. A call center employee appears to have been capturing certain customers' names and debit card information for unauthorized purposes. Upon learning of the incident, we launched an investigation, terminated the employee and reported the issue to law enforcement authorities.

Attribution 1 Publication: MD AG's office Author:
Article Title: Kohl's
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260692.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-16	University of Connecticut	CT	8/5/2015	Electronic	Educational	Yes - Unknown #	Unknown

A vendor that UConn uses to store and manage certain UConn financial data left an FTP portal open and available via a publicly facing website, rather than behind password protection. The fact that this site was left unprotected came to the University's attention when an individual did a Google search on his/her own name and a website popped up that appeared to contain University data. As part of the University's investigation into what data was left unprotected it was determined that a spreadsheet on that open portal contained internal accounting information between University departments.

Attribution 1 Publication: MD AG's office Author:
Article Title: University of Connecticut
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257983.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-15	LPL Financial / Independent Financial Partners	CA	10/21/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On October 8, 2015, we became aware that an Independent Financial Partners/LPL Financial advisor's laptop was stolen while he was attending an offsite meeting. As a result, personal client information, including name, date of birth, Social Security number, and LPL Financial account numbers, may have been exposed.

Attribution 1 Publication: MD AG's office Author:
Article Title: LPL Financial / Independent Financial Partners
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260751.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-14	Intuit's TurboTax Business	CA	10/27/2015	Electronic	Business	Yes - Unknown #	Unknown

Upon discovering this unauthorized access, Intuit immediately investigated and took steps to secure the customers' information. Intuit has determined that unknown individual(s) may have accessed these customer accounts between approximately September 18, 2015 and September 25,2015, by using legitimate credentials obtained elsewhere to access the customers' accounts.

Attribution 1 Publication: MD AG's office Author:
Article Title: Intuit's TurboTax Business
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260747.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-13	Summit Chemical Profit Sharing & 401(K) Plan /	PA	8/17/2015	Electronic	Business	Yes - Unknown #	Unknown

On August 10, 2015, Ascensus, the record keeper for the Summit Chemical Profit Sharing & 401(K) Plan, inadvertently uploaded reports containing names, addresses, birth dates, and Social Security numbers to the secure File Transfer Site of another Ascensus retirement plan client. Upon discovering this, Ascensus immediately informed the recipients that they had received confidential data in error. The client's plan administrator confirmed to Ascensus in writing that they deleted the reports immediately upon identifying that it did not relate to participants in their plan.

Attribution 1 Publication: MD AG's office Author:
Article Title: Summit Chemical Profit Sharing & 401(K) Plan / Ascensus
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-258001.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-12	Interline Brands	FL	8/22/2015	Electronic	Business	Yes - Unknown #	Unknown

On August 7, 2015, we learned that one of our servers, containing information of a limited number of our employees, was compromised on August 5, 2015 by an unauthorized party, and you have been identified as one of a limited number of individuals whose information could possibly have been accessed as a result of this incident. The types of personal information that could have been accessed during this incident include: name, address, phone number, date of birth, and Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Interline Brands
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257930.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-11	Wm. T. Burnett & Co./STX	MD	8/21/2015	Electronic	Business	Yes - Unknown #	Unknown

On June 11, 2015, we were advised by the company that developed and maintains our e-commerce website that it had identified a suspicious file. We immediately contacted the company that hosts our ecommerce website and the file was removed. Those two companies reported that they believe an unauthorized person found a way to remotely insert the file and that the file contained code that was designed to redirect payment card information entered by purchasers on our website to a server accessible by the unauthorized person.

Attribution 1 Publication: MD AG's office Author:
Article Title: Wm. T. Burnett & Co./STX
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257929.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-10	Fidelity Investments	MA	8/27/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Due to an administrative error at Fidelity, another financial advisory firm that holds customer accounts with Fidelity was inadvertently associated with your account ending in XXXX on our systems from December 29, 2008 to August 3, 2015. As a result, the financial advisory firm had access to information about you and your account via a Fidelity proprietary secure website. Additionally, that information was electronically transmitted to a financial institution with whom the financial advisory firm does business.

Attribution 1 Publication: MD AG's office Author:
Article Title: Fidelity Investments
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257926.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-09	Aon Hewitt	IL	8/27/2015	Paper Data	Business	Yes - Unknown #	Unknown

We are writing to notify you that an incident occurred on or around July 15th , 2015. Due to a manual mailing error, information about you, including your name, date of birth, social security number, and pensionspecific information (such as average salary, service, and accrued benefit), was sent to an unintended recipient.

Attribution 1 Publication: MD AG's office Author:
Article Title: Aon Hewitt
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257925%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-08	**Follett Corporation**	IL	8/10/2015	Electronic	Business	Yes - Unknown #	**Unknown**

On or about Thursday, July 23, 2015, Follett learned that the security of certain personally identifiable information housed on the company's online retail ecommerce platform, eFollett.com, may have been compromised. Upon becoming aware of the unauthorized access, Follett immediately took actions to secure the website. We also notified the FBI and engaged recognized security consultants to investigate the unauthorized access.

Attribution 1 Publication: MD AG's office Author:
Article Title: Follett Corporation
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-256839.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-07	**Newton Running**	CO	8/11/2015	Electronic	Business	Yes - Unknown #	**Unknown**

The data security incident occurred on Newton Running's web site. The initial point of compromise occurred between the dates of April 26, 2015 and May 5, 2015. The compromise was contained on May 18, 2015. This incident may have compromised some Massachusetts residents' personal data. We were made aware of this situation when Nexcess, Newton Running's web hosting provider, indicated that there was a potential security incident in the Newton Running environment. The concern was raised when unusual code was found on a production web server.

Attribution 1 Publication: MD AG's office Author:
Article Title: Newton Running
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-256837.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-06	**Department of Human Services Agency**	MD	8/18/2015	Paper Data	Government/Military	Yes - Unknown #	**Unknown**

We are writing to notify you that a letter containing some of your personal information was mistakenly sent to the wrong address. The letter meant for you was inadvertently stuck to another letter and mailed to the wrong individual. When the mistake was discovered, the letter was returned to us immediately. The letter included your name and home address, as well as your case number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Department of Human Services Agency
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-256832.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-05	**New Enterprise Associates / Collected Intelligence LLC**	MD	8/3/2015	Electronic	Business	Yes - Unknown #	**Unknown**

NEA engaged Collected Intelligence to perform due diligence on prospective NEA portfolio company executives and management teams. Collected Intelligence has reported to us that in early June, a password-protected laptop that contained your information was stolen from the home of a Collected Intelligence employee. Collected Intelligence has reported the crime to the police, and has told us that the password-protected laptop contained basic identifying information collected from a discrete number of prospective NEA portfolio company executives, including names and social security numbers. For some individuals, this information also included the date of birth, driver's license number, and address.

Attribution 1 Publication: MD AG's office Author:
Article Title: New Enterprise Associates
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257936.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-04	YMCA of Greater Pittsburgh	PA	7/23/2015	Electronic	Business	Yes - Unknown #	Unknown

On June 8, 2015, YMCA discovered that personal information stored at their Cloverleaf facility may have been exposed after employee files were inadvertently placed in a recycling bin behind the Cloverleaf building by a staff member who did not follow their guidelines for disposing of these documents in a secure manner. The documents were placed in the recycling bin on the evening of June 7, 2015, and recovered the morning of June 8, 2015. Upon review, it appears the documents may have included employees' name, address, date of birth, Social Security number, driver's license number, and other employment-related information. These documents are now secure.

Attribution 1 Publication: MD AG's office Author:
Article Title: YMCA of Greater Pittsburgh
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257935.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151124-03	Good Care Pediatric LLP	NY	11/12/2015	Electronic	Medical/Healthcare	Yes - Published #	2,300

Good Care Pediatric, LLP NY Healthcare Provider 2300 11/12/2015 Hacking/IT Incident Desktop Computer

Attribution 1 Publication: hhs.gov Author:
Article Title: Good Care Pediatric 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
ITRC20151124-02	Healthpoint	WA	11/13/2015	Electronic	Medical/Healthcare	Yes - Published #	1,300

HealthPoint WA Healthcare Provider 1300 11/13/2015 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Healthpoint
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
ITRC20151124-01	W.W. Grainger, Inc.	IL	10/27/2015	Electronic	Business	Yes - Unknown #	Unknown

At Grainger, we take data privacy and security very seriously. As part of a system review, Grainger's IT team recently identified a coding error in the Grainger.com mobile apps for iPhone and Android that resulted in the collection and storage of unsecured user names and passwords on the Grainger system. We learned on October 27, 2015 that the information was inadvertently stored in a system file that was at potential risk of unauthorized access

Attribution 1 Publication: CA AG's office Author:
Article Title: W.W. Grainger, Inc.
Article URL: https://oag.ca.gov/system/files/Sample%20Notice%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151123-01	Starwood Hotels & Resorts Worldwide	CT	11/21/2015	Electronic	Business	Yes - Unknown #	Unknown

Starwood Hotels & Resorts Worldwide Inc. is the latest known hotel target of cyber attackers. The company on Friday announced that hackers had injected malware into point of sale systems at some of its hotels in North America. That malware ultimately made it possible for unauthorized parties to tap into the payment card data Relevant Products/Services of some hotel guests. Starwood, which operates brands including Four Points by Sheraton, Aloft, Element, and Westin, now joins the Trump Hotel Collection and the Hilton chain of hotels on the list of hotel data breaches.

Attribution 1 Publication: CIO-today.com Author: Jennifer LeClaire
Article Title: Some Starwood Hotels Payment Systems Breached
Article URL: http://www.cio-today.com/article/index.php?story_id=112003V3SRQ8

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-13	**Columbia Threadneedle Investments**	MA	11/10/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

I am writing to make you aware of a situation involving your personal information. On October 12, 2015, a scanning error occurred with our vendor and your Future Scholar paperwork which was inadvertently scanned and uploaded to a different investment advisory firm. The investment advisory firm reported the error to our mutual vendor and they immediately corrected the error. We believe this situation poses an extremely low risk, however, the personal information thay may have been viewed included your name and Social Security number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Columbia Threadneedle Investments
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/columbia-threadneedle-investments-20151110.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-12	**Philadelphia Gas Works**	PA	11/11/2015	Electronic	Business	Yes - Unknown #	**Unknown**

On October 1, 2015, we learned that one of our customer service representatives accessed and misused information relating to several PGW customers in order to make improper personal charges or purchases. We immediately began a comprehensive investigation of this incident, disabled the employee's system access and reported the incident to law enforcement. Although we are unaware of any misuse of your account information, we wanted to make you aware of these circumstances, because this customer service representative may have worked on your PGW account while employed at PGW. The information potentially accessed by the employee may have included your name, address, date of birth, Social Security number, driver's license number and your credit, debit or banking information.

Attribution 1 Publication: VT AG's office Author:
Article Title: Philadelphia Gas Works
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Philadelphia%20Gas%20Works%20SBN%20to%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-11	**Boston University**	MA	11/4/2015	Electronic	Educational	Yes - Unknown #	**Unknown**

I am writing to inform you of a data security incident at Boston University related to your participation in the Boston University Initiative for Literacy Development ("BUILD") program through the University's School of Education. Boston University recently learned that an email account connected with the BUILD program was accessed without authorization. That account contained certain forms related to the Boston Public Schools' criminal background check process for participants in the BUILD program (the "CORI forms"), one of which included your name, social security number and driver's license number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-10	**Brandeis University**	MA	11/12/2015	Electronic	Educational	Yes - Unknown #	**Unknown**

Two Apple laptops containing academic and personal information for all students enrolled or taking a course at the University from the summer of 2012 to the present were stolen from the University Registrar, according to a Nov. 12 email sent by Marianne Cwalina, the senior vice president for finance and treasurer. One of the stolen computers contained students' "names, birth dates, permanent and email addresses, phone numbers, courses, and grades," according to Cwalina's email, which went out to students, faculty and staff. "It is also possible that this device contained some Social Security numbers," according to the email.

Attribution 1 Publication: databreaches.net / VT AG's office Author:
Article Title: Theft of two registrar's laptops put Brandeis University students' data at risk
Article URL: http://www.databreaches.net/ma-theft-of-two-registrars-laptops-put-brandeis-university-students-data-at-risk/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-09	**Common Market**	ME	11/13/2015	Electronic	Business	Yes - Unknown #	**Unknown**

We recently learned that there has been a breach of Debit and Credit Card data in our area. The Common Market was one of the stores compromised. Please keep a close eye on your Debit and/or Credit Card transactions for the last couple of months (from August 12 to October 26) for any suspicious activities or charges that you do not recognize. Contact your bank immediately if you see any suspicious activity.

Attribution 1 Publication: databreaches.net Author:
Article Title: Common Market in Maine notifies customers of payment card breach
Article URL: http://www.databreaches.net/common-market-in-maine-notifies-customers-of-payment-card-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-08	Department of Insurance	IL	11/13/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

The Illinois Department of Insurance announced an inadvertent data release, that exposed critical personal information. According to a news release, the department received a complaint that Social Security numbers from a health care provider could be seen. The department says it had sent filings from Blue Cross Blue Shield to the System for Electronic Rate and Form Filing (SERFF) database, which posted the information on its publicly available website.

Attribution 1 Publication: databreaches.net Author:
Article Title: Illinois data breach: Dept. of Insurance posts personal information on public website
Article URL: http://www.databreaches.net/illinois-data-breach-dept-of-insurance-posts-personal-information-on-public-website/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-07	Arthur Brisbane Child Treatment Center	NJ	11/13/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Inside the former Arthur Brisbane Child Treatment Center sat piles of cardboard boxes, turning the former psychiatric hospital into a makeshift storage facility. The files contained within run the gamut of both state employees and Brisbane patients, including personal information such as Social Security numbers, medical history and banking information.

Attribution 1 Publication: databreaches.net / Asbury Park Press Author:
Article Title: Personal records left unprotected at shuttered Brisbane center
Article URL: http://www.databreaches.net/nj-personal-records-left-unprotected-at-shuttered-brisbane-center/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-06	Swiss Cleaners	CT	11/16/2015	Electronic	Business	Yes - Unknown #	Unknown

Swiss Cleaners values the relationship it has with its customers and understands the importance of protecting payment card information. Swiss Cleaners was recently notified that banks had identified a pattern of unauthorized charges on payment cards after those cards were used in Swiss Cleaners stores. Swiss Cleaners immediately began to investigate and engaged a leading computer security firm to examine its payment system.

Attribution 1 Publication: databreaches.net / Scmagazine.com Author:
Article Title: Alerted that banks had discovered a problem, Swiss Cleaners investigates and notifies customers of payment card breach that
Article URL: http://www.databreaches.net/ct-alerted-that-banks-had-discovered-a-problem-swiss-cleaners-investigates-and-notifies

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-05	City of Tampa	FL	11/18/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

The city broke federal law and put some workers at risk of identity theft by including their Social Security numbers on child support and other garnishment checks, a city audit found. The audit of the city's Accounts Payable department showed Social Security numbers were printed on payment checks sent to banks, creditors and other recipients and also on remittance advice slips kept on file. That violates the 2010 Social Security Number Protection Act, which prohibits government agencies using the number on any check or payment.

Attribution 1 Publication: tbo.com / databreaches.net Author:
Article Title: Audit finds Tampa put city workers at risk of ID theft
Article URL: http://www.tbo.com/news/politics/audit-finds-tampa-put-city-workers-at-risk-of-id-theft-20151117/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-04	Quest Diagnostics	NJ	11/17/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A Brooklyn marketing office was inundated for months by hundreds of private medical documents meant for Quest Diagnostics, but couldn't get anyone at the clinical laboratory services company to take action until she called NBC 4 New York's I-Team. The faxes were all medical papers, with sensitive information, including name, date of birth, phone numbers, and sometimes social security numbers for patients. They almost always included the type of the test that was being ordered for the individuals and were faxed from many different medical offices in the New York metropolitan area

Attribution 1 Publication: NBC4 New York / databreaches.net Author:
Article Title: I-Team: Hundreds of Personal Medical Records Intended for Lab Sent to Brooklyn Marketing Firm in Error
Article URL: http://www.nbcnewyork.com/news/local/Medical-Records-Mix-up-Investigation-Doctor-Privacy-351060331.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-03	Georgia Secretary of State	GA	11/18/2015	Electronic	Government/Military	Yes - Published #	6,000,000

Two Georgia women have filed a class action lawsuit alleging a massive data breach by Secretary of State Brian Kemp involving the Social Security numbers and other private information of more than six million voters statewide. The suit, filed Tuesday in Fulton County Superior Court, alleges Kemp's office released the information including personal identifying information to the media, political parties and other paying subscribers who legally buy voter information from the state.

Attribution 1 Publication: ajc.com Author:
Article Title: Suit accuses Georgia of massive data breach involving 6 million voters
Article URL: http://www.ajc.com/news/news/state-regional-govt-politics/suit-accuses-georgia-of-massive-data-breach-involv/npQL

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-02	Securus Technologies	TX	11/13/2015	Electronic	Business	Yes - Published #	63,000

Reporters at The Intercept recently received a 37 GB cache of records of more than 70 million phone calls apparently stolen from Securus Technologies, which provides phone services for approximately 2,200 U.S. prisons. The calls were placed between December 2011 and the spring of 2014 -- the records include calls placed to almost 1.3 million unique phone numbers by more than 63,000 inmates.

Attribution 1 Publication: eSecurityplanet.com Author:
Article Title: Breach at Securus Technologies Exposes 70 Million Prison Phone Calls
Article URL: http://www.esecurityplanet.com/network-security/breach-at-securus-technologies-exposes-70-million-prison-phone-ca

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151118-01	LTC Dental, PC	AL	10/28/2015	Electronic	Medical/Healthcare	Yes - Published #	1,680

LTC Dental, P.C .AL Healthcare Provider 1680 10/28/2015 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: LTC Dental, 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
ITRC20151116-04	Dean Health	WI	11/12/2015	Electronic	Medical/Healthcare	Yes - Published #	960

Madison, Wis.-based insurance company Dean Health is reporting a breach of protected health information that may affect 960 patients, after documents mailed to a bank were lost, according to the Wisconsin State Journal.

Attribution 1 Publication: beckershospitalreview.com Author: Max Green
Article Title: Documents lost in the mail trigger breach impacting 960 Dean Health Plan members
Article URL: http://www.beckershospitalreview.com/healthcare-information-technology/documents-lost-in-the-mail-trigger-breach-i

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151116-03	OH Muhlenberg, LLC	KY	11/16/2015	Electronic	Medical/Healthcare	Yes - Published #	84,681

Friday, Owensboro Health Muhlenberg, LLC announced that its hospital in Greenville, KY, experienced a security incident affecting some of the hospital's computers. Hospital officials say they were notified by the FBI in September of suspicious network activity involving third parties. Officials say the hospital responded by initiating an internal investigation and hiring a digital forensics and security firm to investigate. We're told they discovered "a limited number" of computers were indeed infected with a keystroke logger designed to capture and transmit data as it was entered onto the affected computers.

Attribution 1 Publication: hipaajournal.com / databreaches.net Author: 11/17/2015
Article Title: Major Data Exfiltration Discovered at Muhlenberg Community Hospital
Article URL: http://www.hipaajournal.com/major-data-exfiltration-discovered-at-muhlenberg-community-hospital-8183/

Attribution 2 Publication: 14News / WFIE Author:
Article Title: Owensboro Health says Greenville hospital experienced security breach
Article URL: http://www.14news.com/story/30527902/owensboro-health-says-greenville-hospital-experienced-security-breach

Attribution 3 Publication: databreaches.net Author:
Article Title: FBI alerts Owensboro Health to Breach at Muhlenberg Hospital; Breach Began in January, 2012
Article URL: http://www.databreaches.net/fbi-alerts-owensboro-health-to-breach-at-muhlenberg-hospital-breach-began-in-january-2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151116-02	University of Cincinnati Medical Center	OH	11/16/2015	Electronic	Medical/Healthcare	Yes - Published #	1,064

After an emailing error, the University of Cincinnati Medical Center has announced a health data breach potentially compromising the PHI of 1,064 individuals. Starting in 2014, the medical center experienced nine incidents of emailing private patient information to the wrong email address, according to a hospital statement. While the hospital reportedly intended to send the emails to employees within the hospital network, UC Health workers swapped two letters in the domain name, thus inadvertently sending the emails to someone potentially not within the hospital system. UC Health discovered this error on September 16, 2015.

Attribution 1 Publication: healthitsecurity.com Author:
Article Title: UC Medical Center Email Typo Results in PHI Data Breach
Article URL: http://healthitsecurity.com/news/uc-medical-center-email-typo-results-in-phi-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151116-01	Department of Health and Human Services #2	NC	11/16/2015	Electronic	Government/Military	Yes - Published #	524

For the second time in two months, the North Carolina Department of Health and Human Services (DHHS) has experienced a health data breach due to an improperly encrypted email, according to WRAL.com. The incident, which occurred in September, involves the health data of 524 state Medicaid patients. Although DHHS reports that the email that compromised the information was sent to the correct recipient, there is still the risk that the email was intercepted. However, DHHS added it has no reason to believe that the email was intercepted.

Attribution 1 Publication: healthitsecurity.com Author:
Article Title: An unencrypted email potentially disclosed health information for over 500 patients in North Carolina.
Article URL: http://healthitsecurity.com/news/dhhs-has-second-email-health-data-breach-in-two-months

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151113-01	Fashion to Figure	DE	10/16/2015	Electronic	Business	Yes - Unknown #	Unknown

Fashion to Figure (B. Lane, Inc.) is notifying customers of a breach involving malware inserted on their web host's server. The malware was reportedly inserted on the unnamed host's server on May 19, but Fashion to Figure did not realize it until October 16, when they started investigating why a web page was loading slowly.

Attribution 1 Publication: CA AG's office / Databreaches.net Author:
Article Title: Fashion to Figure notifying customers of payment card compromise
Article URL: http://www.databreaches.net/fashion-to-figure-notifying-customers-of-payment-card-compromise/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151112-01	Comcast	AL	11/12/2015	Electronic	Business	Yes - Unknown #	Unknown

US mass media giant Comcast has denied allegations of a data breach after email addresses and passwords of more than 590,000 customers went on sale in the dark web

Attribution 1 Publication: CBRonline.com Author:
Article Title: Comcast dodges blame for customer data breach hack
Article URL: http://www.cbronline.com/news/cybersecurity/data/comcast-dodges-blame-for-customer-data-breach-hack-4717112

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151110-01	Rush University Medical Center	IL	11/6/2015	Paper Data	Medical/Healthcare	Yes - Published #	1,529

A minor data disclosure affected a limited number of patients of Paul Jones, MD. Letters were sent to the patients announcing the retirement of their physician. The letters were sent to the right addresses, although they included the name of an incorrect patient.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Rush University Medical Center
Article URL: http://www.hipaajournal.com/another-hipaa-breach-courtesy-of-a-printing-error-8205/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151109-04	HUNTINGTON MEDICAL RESEARCH INSTITUTE #2	CA	11/5/2015	Electronic	Medical/Healthcare	Yes - Published #	4,300

The second incident was discovered two weeks later to the day. HMRI has not confirmed that the employee in question definitely took some Protected Health Information of patients, although the company does believe this to be the case. The exact same data types were exposed: patient names, dates of birth, demographic data, diagnosis and treatment information, specimen information, tissue source, tests ordered, and the referring physician's name.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Alleged Theft of Patient Data by Former Employee
Article URL: http://www.hipaajournal.com/huntington-medical-research-institutes-discovers-two-hipaa-breaches-8174/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151109-03	Four Winds Casino Resort	MI	11/6/2015	Electronic	Business	Yes - Unknown #	Unknown

The investigation found evidence of a criminal attack on its payment card network that involved the installation of a program that searched for payment card data as it was being routed through its network. The program specifically searched for data found in the magnetic stripe of payment cards, which includes the cardholder name, card number, expiration date and internal verification code. No other customer information was involved.

Attribution 1 Publication: Four Winds Casino website Author:
Article Title: Four Winds Casino Resort Identifies and Stops Payment Card Incident
Article URL: http://fourwindscasino.com/press/payment-card.php

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151109-02	Utah State Office of Education	UT	11/5/2015	Electronic	Educational	Yes - Published #	5,500

On 4th November 2015 we received information confirming that Touchnote has been the victim of criminal activity, resulting in the theft of some of our customer data. As a part of the investigation, which is continuing, we have found that some of the customer information stolen included names, email addresses, postal addresses, and Touchnote order histories. There have also been some recorded instances of dates of birth being accessed.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Utah student information compromised over six-year period
Article URL: http://www.scmagazine.com/utah-student-information-compromised-over-six-year-period/article/452046/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151109-01	Department of Motor Vehicles	CA	10/9/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

On September 28, 2015, a DMV employee was sending a file containing your personal information to the Santa Clara Transportation Agency as part of the agency's Employer Pull Notice (EPN) program. The EPN program provides agencies with a means of promoting driver safety through the ongoing review of driver records.

Attribution 1 Publication: CA AG's office Author:
Article Title: Department of Motor Vehicles
Article URL: https://oag.ca.gov/system/files/Notice%201_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151105-04	Huntington Medical Research Institutes #1	CA	10/20/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

On August 6, 2015, HMRI discovered paper records and glass laboratory microscope slides had been disposed of in a way that did not comply with HIPAA regulations. The incident is believed to have occurred at some point in the two weeks prior to HMRI becoming aware of the HIPAA breach.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Insecure Disposal of Laboratory Slides and Medical Files Discovered
Article URL: http://www.hipaajournal.com/huntington-medical-research-institutes-discovers-two-hipaa-breaches-8174/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151105-03	Maryland Department of Information Technology	MD	11/4/2015	Electronic	Government/Military	Yes - Published #	500

Maryland's Department of Information Technology is admitting to exposing the "Personally Identifiable Information" of hundreds of people and companies that do business with the state by accidentally publishing a list of them on a public website. Data exposed included Social Security and Tax ID numbers.

Attribution 1 Publication: WUSA9.com Author:
Article Title: Maryland admits to exposing personal information of hundreds
Article URL: http://www.wusa9.com/story/news/local/maryland/2015/11/04/maryland-admits-exposing-personal-information-of-hund

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151105-02	Interstitial Cystitis Network (ICN Mail Order Center)	CA	10/26/2015	Electronic	Business	Yes - Unknown #	Unknown

We first learned of a possible breach when two customers contacted our office to report that their credit card information may have been compromised. In both cases, they first experienced a fraudulent charge on Facebook. We immediately performed a security review of our server and are confident that the breach did not occur in our offices or the systems that we directly maintain. Our investigation revealed that the breach occurred through the use of a password stolen from one of our vendor

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: Interstitial Cystitis Network (ICN Mail Order Center)
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Interstitial%20Cystitis%20Network%20SBN%20to%20C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151105-01	Avis Budget Group	NJ	10/6/2015	Electronic	Business	Yes - Unknown #	Unknown

On October, 2, 2015 thethird-party provider, which manages our benefits open enrollment process, inadvertently sent a file containing personal information, which included your name,address and social security number, to another company tha tis also one of its clients.

Attribution 1 Publication: CA AG's office Author:
Article Title: Avis Budget Group
Article URL: https://oag.ca.gov/system/files/Employee%20Notification%20Letter%20-%20Final%20%282%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151103-03	Dow Corning Corporation	MI	10/30/2015	Electronic	Business	Yes - Published #	4,000

The incident arose because two contractors of one of our vendors who had access to employee data as a part of their interaction with us took a number of documents upon their termination. The personal information involved included names, contact informacion, financial information (such as salary information and some bank account numbers), Social Security Numbers and non-HIPAA related benefit enrollment information.

Attribution 1 Publication: ourmidland.com Author:
Article Title: Some unhappy with Dow Corning's response to data breach
Article URL: http://www.ourmidland.com/news/some-unhappy-with-dow-corning-s-response-to-data-breach/article_0b8d0bd9-0006-

Attribution 2 Publication: NH AG's office Author:
Article Title: Dow Corning Corporation
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/dow-corning-20151030.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151103-02	BeHealthy Health Plan	FL	11/2/2015	Paper Data	Medical/Healthcare	Yes - Published #	835

Florida-based BeHealthy Health Plan has inadvertently exposed the health insurance claim numbers of 835 subscribers after a mailing error resulted in the data being printed on the outside of envelopes. The mailing of benefit information packets took place on September 23, 2015, with the first complaints alerting the health plan to error being received 5 days later. The privacy breach affects members of the BeHealthy Medicare Advantage Plan who live in Manatee and Sarasota counties.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: BEHEALTHY MAILING ERROR SEES PHI PRINTED ON OUTSIDE OF ENVELOPES
Article URL: http://www.hipaajournal.com/behealthy-mailing-error-sees-phi-printed-on-outside-of-envelopes-8168/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151103-01	Accuform Signs	FL	9/21/2015	Electronic	Business	Yes - Unknown #	Unknown

We are contacting you regarding a data security incident that has occurred at Accuform Signs. Essentially, our systems have been illegally hacked into by outside intruders. Beginning at least as early as June 30, 2015, we believe Accuform Signs order information was improperly accessed from our website and/or the website of [DISTRIBUTOR NAME] (with whom we are working closely in order to provide you this joint notification with important information to better protect you). This order information may have included your name, address, email, phone and credit card information. As a result, this information may have been potentially exposed to others

Attribution 1 Publication: CA AG's office Author:
Article Title: Accuform Signs
Article URL: https://oag.ca.gov/system/files/Accuform-SampleNotification%20-%20Standard_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151030-05	Wisconsin Department of Veterans Affairs	WI	10/30/2015	Electronic	Government/Military	Yes - Published #	637

The Social Security numbers of Wisconsin veterans are being sent via email without encryption despite numerous federal laws and U.S. Department of Veterans Affairs regulations requiring personally identifiable information be password-protected. It partly explains how a random Wisconsin veteran received an unsolicited email on April 1 with the Social Security numbers and disability claim information of hundreds of Wisconsin veterans. Since the Vietnam War, veterans' file numbers or disability claim numbers have been their Social Security numbers.

Attribution 1 Publication: Channel3000.com Author: Adam Schrager
Article Title: Veteran receives email listing hundreds of Social Security numbers
Article URL: http://www.channel3000.com/news/veteran-receives-email-listing-hundreds-of-social-security-numbers/36124636

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151030-04	OsteoMed LP	TX	10/20/2015	Electronic	Medical/Healthcare	Yes - Published #	1,134

OsteoMed recently learned that a former employee improperly copied a set of Human Resources forms and manuals from company systems when the individual was terminated in January, 2015. The files contained the personal information of current and former OsteoMed employees and their dependents, including names, addresses, Social Security numbers, dates of birth, employee identification numbers, and health insurance elections. The documents also contained certain other HR information, such as employment, compensation, and tax-related information.

Attribution 1
Publication: hhs.gov / MD AG's office Author:
Article Title: OsteoMed LP
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-260752.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151030-03	Children's Medical Clinics of East Texas	TX	10/28/2015	Electronic	Medical/Healthcare	Yes - Published #	16,000

A Children's Medical Clinics of East Texas employee was discovered to have removed business documents and taken them home, and failed to return them when requested to do so. Following this incident an internal investigation was conducted which revealed the employee had also accessed patient medical records without authorization, and had taken a copy of the data and gave it to another "disgruntled ex-employee," although the identity of that individual was not disclosed to the healthcare provider.

Attribution 1
Publication: hhs.gov / hipaajournal.com Author:
Article Title: 16K CHILDREN'S MEDICAL RECORDS POTENTIALLY STOLEN IN EAST TEXAS
Article URL: http://www.hipaajournal.com/16k-childrens-medical-records-potentially-stolen-in-east-texas-8178/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151030-02	Woodhull Medical and Mental Health Center / NY	NY	10/28/2015	Electronic	Medical/Healthcare	Yes - Published #	1,581

The New York City Health and Hospitals Corporation (HHC) has sent breach notification letters to 1,581 patients of its Brooklyn Woodhull Medical and Mental Health Center, after a laptop computer was discovered to have been stolen. The laptop computer was password protected, but data stored on its hard drive had not been encrypted. As a result, the Protected Health Information of some of its patients could potentially have been compromised.

Attribution 1
Publication: hipaajournal.com Author:
Article Title: Woodhull Medical and Mental Health Center Data Breach Announced
Article URL: http://www.hipaajournal.com/woodhull-medical-and-mental-health-center-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151030-01	Yellowfront Grocery	ME	10/29/2015	Electronic	Business	Yes - Unknown #	Unknown

Yellowfront Grocery in Damariscotta, Maine, notified its customers via Facebook that it had experienced a point-of-sale (POS) breach on Oct 23. How many victims? Undetermined. But two banks have issued 3,000 replacement payment cards in response to the breach. What type of information? Yellowfront Grocery store owner Jeff Pierce told SCMagazine.com that he is certain payment card numbers were compromised but is unsure if additional information was stolen.

Attribution 1
Publication: scmagazine.com Author:
Article Title: Maine's Yellowfront Grocery hit by breach, other stores may be affected
Article URL: http://www.scmagazine.com/yellowfront-grocery-notified-customers-via-facebook-of-pos-breach/article/450345/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151029-04	ShowTix4U / Digital Theatre, LLC	NV	10/9/2015	Electronic	Business	Yes - Unknown #	Unknown

Although our independent forensic investigation is ongoing, at this time, we believe that between late April 2015 and late September 2015 unauthorized individuals installed malicious software on a computer server hosting the Website. According to our records, you made a payment card purchase on the Website during that timeframe and your information may be at risk. While Digital Theatre does not store credit card information, we believe the malware could have compromised the personal information (name, address, payment card account number, card expiration date, and payment card security code) of customers that made credit card purchases through the Website.

Attribution 1 Publication: CA AG's office Author:
Article Title: ShowTix4U / Digital Theatre, LLC
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_2.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151029-03	STILETTO Solutions	CA	9/16/2015	Electronic	Business	Yes - Unknown #	Unknown

We wanted to make you aware of recent unauthorized access to STILETTO Solutions cardholder payment data, including yours. After identifying suspicious activity within our e-Commerce server, our incident response team began to investigate the incident as soon as we learned of it. Working with our forensic investigators and IT security advisors, we have learned that certain customer credit card information might have been acquired by an unauthorized party from our STILETTO Solutions server. The compromise of our e-Commerce server occurred on September 16, 2015 and may impact the security of credit and debit cards customers used for purchases through our site, stilettosolutions.com, from November 1, 2013 through and including September 16, 2015.

Attribution 1 Publication: CA AG's office Author:
Article Title: STILETTO Solutions
Article URL: https://oag.ca.gov/system/files/STILETTO%20-%20Notice%20Letter_Final%20%285772563x7AB84%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151029-02	Woodhull Medical and Mental Health Center	NY	10/28/2015	Electronic	Medical/Healthcare	Yes - Published #	1,500

A New York City medical and mental health center recently reported a potential PHI data breach after a laptop containing patient information was stolen, underscoring the importance of encrypting devices on which patient health data is stored. The laptop belonged to Woodhull Medical and Mental Health Center, a part of the New York City Health and Hospitals Corporation (HHC). According to a health data breach notification letter, the laptop had been stolen from a patient exam room between the night of August 18, 2015 and the afternoon of August 19, 2015.

Attribution 1 Publication: healthitsecurity.com Author:
Article Title: NYC Health Center Notifies 1,500 Patients of PHI Data Breach
Article URL: http://healthitsecurity.com/news/nyc-health-center-notifies-1500-patients-of-phi-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151029-01	Casey's General Stores	IA	10/28/2015	Electronic	Business	Yes - Unknown #	Unknown

There's been a security breach in the Midwest that could involve your credit card information. Casey's general stores said it has found "credit card skimming devices" on the fuel pumps at seven of its stores, one of them here in the Quad Cities.

Attribution 1 Publication: KWQC TV 6 Author:
Article Title: Tips to keep your identity safe after security breach at Davenport Casey's General Store
Article URL: http://kwqc.com/2015/10/28/tips-to-keep-your-identity-safe-after-security-breach-at-davenport-caseys-general-store/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151027-02	Osceola County	FL	10/21/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

9 Investigates uncovered an error that allowed personal information of children in Osceola County to go public. Juvenile records are never accessible to the public to protect children. That's why a sign in front of the clerk's office says, "Juvenile cases are confidential." Reyes found names for every child charged in and names of children in foster care in Osceola County.

Attribution 1 Publication: wftv.com Author:
Article Title: 9 Investigates: Osceola County children's personal information posted online
Article URL: http://www.wftv.com/news/news/local/9-investigates-osceola-county-childrens-personal-i/nn7QF/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151027-01	EnvisionRx	OH	10/23/2015	Paper Data	Medical/Healthcare	Yes - Published #	540

An error occurred when exporting data from a PDF file for a prescription mailing, resulting in 540 patients (out of a mailing of 11,000 letters) being sent data relating to other patients. The PHI exposed in this HIPAA breach included patient names, drug/dosage information, dates of service, prescription costs, and copay/plan payment amounts.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: EnvisionRx
Article URL: http://www.hipaajournal.com/another-hipaa-breach-courtesy-of-a-printing-error-8205/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151026-07	Health Care Service Corporation	IL	9/17/2015	Paper Data	Medical/Healthcare	Yes - Published #	501

Health Care Service Corporation IL Health Plan 501 09/17/2015 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Health Care Service Corporation
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=5E9297C5A25E70F401A1318AFC6F3B67.ajp13w

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151026-06	Anne Arundel Health System	MD	10/8/2015	Paper Data	Medical/Healthcare	Yes - Published #	2,208

Anne Arundel Health System MD Healthcare Provider 2208 10/08/2015 Unauthorized Access/Disclosure Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151026-05	Department of Health's Children's Medical Services	FL	10/23/2015	Paper Data	Government/Military	Yes - Published #	500

About 150 clients of the Florida Department of Health's Children's Medical Services program in Miami-Dade may have had their personal information compromised after vendors were faxed a clinic roster containing names, birth dates and membership numbers, agency officials reported Friday.

Attribution 1 Publication: miamiherald.com Author:
Article Title: Miami-Dade patient information compromised
Article URL: http://www.miamiherald.com/news/health-care/article41242278.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151026-04	Emergence Health Network	TX	10/26/2015	Electronic	Medical/Healthcare	Yes - Published #	11,100

EHN became aware of strange activity on one of our computer servers on August 18, 2015. Someone, without permission from EHN, accessed the computer server through an internet connection. Because of the internet, the person or persons could have accessed this computer server from any location. A computer specialist inspected the computer server and found out that the first unapproved access of the server may have happened back in 2012. The information which was kept on the server included your first and last name, address, date of birth, social security number, case number, and information indicating that you accessed services from Life Management Center/ El Paso MHMR/Emergence Health Network.

Attribution 1 Publication: databreaches.net / EHN notification lette Author:
Article Title: Emergence Health Network
Article URL: http://emergencehealthnetwork.org/wp-content/uploads/2015/10/EHN-Computer-Server-compromise-notification-letter

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151026-03	Aspire Home Care and Hospice (Indian Territory	OK	10/22/2015	Electronic	Medical/Healthcare	Yes - Published #	4,500

The perpetrator of the attack first gained access to email accounts in late July, and potentially obtained patient names, dates of birth, Social Security numbers and insurance information, placing the victims at a particularly high risk of suffering identity theft, medical and insurance fraud. (Indian Territory Home Health and Hospice)

Attribution 1 Publication: hipaajournal.com / databreaches.net Author:
Article Title: Aspire Home Care and Hospice Cyberattack Exposes 4,278 Patient Records
Article URL: http://www.hipaajournal.com/aspire-home-care-and-hospice-cyberattack-announced-8160/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151026-02	Bon Secours St. Francis Health System	SC	10/26/2015	Electronic	Medical/Healthcare	Yes - Published #	1,997

An employee at Bon Secours St. Francis Health System has been terminated after hospital officials discovered that she had inappropriately accessed personal patient information. An investigation concluded on Aug. 26 that an employee had been accessing patient medical records "in a manner that was inconsistent with her job functions, hospital procedures and ... training," between Jan. 1, 2014 and Aug. 12, 2015, according to the statement.

Attribution 1 Publication: greenvilleonline.com / hhs.gov Author:
Article Title: Email Error Causes Neuropathology Associates Data Breach
Article URL: http://www.greenvilleonline.com/story/news/2015/10/26/employee-fired-after-st-francis-data-breach/74638284/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151026-01	Noble House Hotel and Resorts - The Commons	WA	9/25/2015	Electronic	Business	Yes - Published #	19,472

Noble House began an investigation after we received calls from some of our guests who saw unauthorized charges on their payment cards used at one of our hotels, The Commons. We notified the FBI regarding the incident. We engaged a computer security firm to examine our payment system for any signs of an issue. The computer security firm identified malware on the payment card system for The Commons on September 25, 2015. The information potentially compromised by the malware included data found in the magnetic stripe on payment cards, which includes the cardholder name, card number, expiration date, and CVV number.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Payment card breach at The Commons Hotel in Minnesota
Article URL: http://www.scmagazine.com/payment-card-breach-at-the-commons-hotel-in-minnesota/article/449159/

Attribution 2 Publication: CA AG's office / databreaches.net Author:
Article Title: Noble House Hotel and Resorts - The Commons
Article URL: https://oag.ca.gov/system/files/General%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151020-08	Santander Bank #5	MA	10/7/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On September 17, 2015, the Santander Bank Fraud Card Detection group discovered suspicious ATM withdrawals that occurred that day. Upon further investigation, it was determined that a magnetic stripe skimming device had been placed on the ATM vest ibule door of our remote ATM located at 495 Southern Artery, Quincy, MA. It is believed that a device was placed on the ATM vestibule door on August 28, 2015 and removed August 28, 2015, and that a device was again placed on the vestibule door on August 29, 2015 and removed August 29, 2015. The personal information potentially compromised included the customer's name, card number, card expiration date, card security code, and
card PIN number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Santander Bank #5
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/santander-20151007.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151020-07	Salt Lake County	UT	10/9/2015	Electronic	Government/Military	Yes - Published #	14,000

On September 9, 2015, Salt Lake County learned of a possible security incident involving Workers' Compensation or other damage claims submitted to the County. Salt Lake County immediately began an investigation into the situation and learned that, on June 18, 2015, a software services company hired by the County improperly set one or more security settings during a scheduled upgrade. While the investigation is ongoing, it appears that the improper settings may have allowed information submitted to the County in connection with Worker's Compensation or other damages claims to be temporarily accessible on the Internet. This information may have included the name, address, limited medical information associated with a claim, and in some cases Social Security numbers of claimants.

Attribution 1 Publication: NH AG's office / scmagazine.com Author:
Article Title: Salt Lake County
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/salt-lake-city-20151009.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151020-06	EyeByeDirect, Inc.	TX	10/13/2015	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you of an incident that may have involved your personal information. On June 16, 2015, we learned that hackers using a Russian IP address gained unauthorized access to EyeBuyDirect's website sometime between February 9 and May 30, 2015. During that time, the hackers may have accessed the personal information of certain customers, including frrst, middle and last names, mailing addresses, shipping addresses, phone numbers, e-mail addresses, credit card numbers & CVV codes (the security code on the back of your card).

Attribution 1 Publication: NH AG's office / scmagazine.com Author:
Article Title: EyeByeDirect, Inc.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/eyebuydirect-20151013.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151020-05	Neuropathology Associates, PLC	AR	10/16/2015	Electronic	Medical/Healthcare	Yes - Published #	1,260

In this instance, the BA of Neuropathology Associates was accidentally sent a limited amount of Protected Health Information (PHI) that was not required. De-identified data were provided, in accordance with HIPAA Rules; however, PHI was also accidentally attached to the email and sent to the BA along with the de-identified data. The data were also sent via unencrypted email.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Email Error Causes Neuropathology Associates Data Breach
Article URL: http://www.hipaajournal.com/email-error-neuropathology-associates-data-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151020-04	Millers Mutual Group	PA	10/16/2015	Electronic	Business	Yes - Unknown #	Unknown

In the past, you brought a claim against a company that was insured by Millers. On September 23, 2015, we learned that some of your claim information, which had been stored on servers used by our claims software vendor ("vendor"), was accessed by an unauthorized individual. The vendor maintained this claims information off-site, without Millers' knowledge or permission. Upon learning of this incident, we immediately began an investigation in cooperation with our vendor, and the incident was reported to law enforcement. Our investigation determined that the claims information stored on the server used by our vendor included your name, address, date of birth, and Social Security number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151020-03	Department of Health and Human Services	NC	10/17/2015	Electronic	Government/Military	Yes - Published #	1,615

The state Department of Health and Human Services says a breach of security protocol may have compromised the confidential health information of 1,615 Medicaid patients. According to the agency, a DHHS employee "inadvertently sent an email to the Granville County Health Department without first encrypting it." The email included a spreadsheet containing protected health information for Medicaid recipients, which the agency says "included the individual's first and last name, Medicaid identification number (MID), provider name and provider ID number, and other information related to Medicaid services."

Attribution 1 Publication: WRAL.com / databreaches.net Author:
Article Title: DHHS reveals potential Medicaid data breach
Article URL: http://www.wral.com/nc-dhhs-reveals-potential-medicaid-data-breach/14975745/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151020-02	Johns Hopkins Medicine	MD	10/20/2015	Electronic	Medical/Healthcare	Yes - Published #	838

Johns Hopkins Medicine reported a physician's missing laptop on August 10, according to a hospital statement. The unencrypted laptop contained health information for 571 cancer patients and 267 study participants.

Attribution 1 Publication: healthitsecurity.com Author:
Article Title: Stolen laptop leads to Johns Hopkins health data breach
Article URL: http://healthitsecurity.com/news/ark.-md.-providers-notify-patients-of-health-data-breaches

Attribution 2 Publication: hipaajournal.com Author:
Article Title: John Hopkins Medicine Data Breach
Article URL: http://www.hipaajournal.com/unencrypted-device-theft-continues-to-plague-hipaa-ces-8158/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151020-01	Baptist Health And Arkansas Health Group	AR	10/20/2015	Electronic	Medical/Healthcare	Yes - Published #	6,500

On October 1, the Baptist Health and Arkansas Health Group notified 6,500 patients that two former employees of the health group had downloaded patient information to take with them to a new practice, Bray Family Health.

Attribution 1 Publication: healthitsecurity.com / hhs.gov Author:
Article Title: Former employees bring patient information to new practice
Article URL: http://healthitsecurity.com/news/ark.-md.-providers-notify-patients-of-health-data-breaches

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151019-03	University of Oklahoma Department of Urology	OK	10/16/2015	Electronic	Medical/Healthcare	Yes - Published #	9,300

What happened? A laptop containing the personal information was stolen from a physician who formerly worked for the University of Oklahoma Department of Urology. What type of personal information? Names, diagnoses and treatment codes and dates, dates of birth or ages, brief descriptions of urological medical treatments or procedures, medical record numbers and treating physician names.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Laptop theft affects thousands of OU Medicine patients
Article URL: http://www.scmagazine.com/laptop-theft-affects-thousands-of-ou-medicine-patients/article/447709/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151019-02	Food.com / Scripps Network	TN	9/16/2015	Electronic	Business	Yes - Unknown #	Unknown

We recently learned of a potential unauthorized intrusion into the Food.com system that may have affected your email/username and password for logging into your Food.com account used for managing your recipe box and posting recipes on the site. These credentials can also be used to log into your user account on the Foodnetwork.com website as well as the Food Network In the Kitchen and Food.com mobile applications. We have been actively working with an experienced cybersecurity forensic investigator to assist with our investigation of the incident.

Attribution 1 Publication: CA AG's office Author:
Article Title: Food.com / Scripps Network
Article URL: https://oag.ca.gov/system/files/Consumer%20Notice_2.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151019-01	Community Catalysts of California	CA	10/16/2015	Electronic	Business	Yes - Published #	1,182

On or about August 31, 2015, the residence of an employee of Community Catalysts of California was burglarized and items were stolen including a flash drive. Community Catalysts was notified of the theft on September 8, 2015. The flash drive may have contained the name, address, diagnosis, date of birth, age, gender and/or telephone number for certain of Community Catalysts of California's current and former clients. The social security numbers for 18 clients may also have been contained on the flash drive. No driver's license, state identification, health insurance or financial account numbers were contained on the flash drive.

Attribution 1 Publication: CA AG's office Author:
Article Title: Community Catalysts of California
Article URL: https://oag.ca.gov/system/files/Letter%20to%20CA%20AG_2.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151015-02	Uber	CA	10/14/2015	Electronic	Business	Yes - Published #	1,182

While it is all well and good that the issue was fixed quickly, the personal data of around 674 drivers was exposed in the United States and those drivers could now potentially be at risk, something that hasn't been addressed by the company. The design flaw in the app also gave drivers more information about each other by allowing anyone access to almost 1,000 sensitive scanned documents, including social security numbers, tax forms, insurance documents, driving licenses and taxi certification forms.

Attribution 1 Publication: dispatchtimes.com Author:
Article Title: UBER SUFFERS MASSIVE SECURITY BREACH, EXPOSES LICENSES & IRS DOCUMENTS
Article URL: http://www.dispatchtimes.com/uber-suffers-massive-security-breach-exposes-licenses-irs-documents-for/132097/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151015-01	Mainstreet Federal Credit Union	KS	10/15/2015	Electronic	Banking/Credit/Financial	Yes - Published #	300

A data breach compromised information belonging to about 300 members of the Lenexa, Kan.-based Mainstreet Federal Credit Union, according to President/CEO John Beverlin. Beverlin told CU Times hackers did not break into the credit union's systems and that the fraudsters likely purchased members' information somewhere online. Now the criminals are trying to capitalize on it, he said, and they've rung up more than $200,000 in fraudulent charges so far.

Attribution 1 Publication: wbap.com Author:
Article Title: Data Breach Hits Mainstreet FCU
Article URL: http://www.wbap.com/2015/10/15/a-data-breach-at-a-popular-dallas-attraction/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151013-08	Humana Medicare Advantage	KY	10/9/2015	Electronic	Medical/Healthcare	Yes - Published #	2,815

Humana reports that about some of their Humana Medicare Advantage accounts may have been stolen. The company said an employee's vehicle was broken into and a secure, encrypted laptop was stolen along with hard copy files. The laptop contained encrypted data on about 2,800 customers. The paper files contained ID numbers for about 250 customers.

Attribution 1 Publication: wisn.com Author:
Article Title: Humana reports data breach that could affect up to 2,800
Article URL: http://www.wisn.com/news/humana-reports-data-breach-that-could-affect-up-to-2800/35754006

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151013-07	America's Thrift Stores	AL	10/12/2015	Electronic	Business	Yes - Unknown #	Unknown

"This breach allowed criminals from eastern Europe unauthorized access to some payment card numbers. This virus/malware is one of several infecting retailers across North America," America's Thrift Stores wrote in a statement. "The U.S. Secret Service tells us that only card numbers and expiration dates were stolen. They do not believe any customer names, phone numbers, addresses or email addresses were compromised."

Attribution 1 Publication: shelbycountyreporter.com Author:
Article Title: America's Thrift Stores report security breach
Article URL: http://www.shelbycountyreporter.com/2015/10/12/americas-thrift-stores-report-security-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151013-06	E*Trade	NY	10/12/2015	Electronic	Banking/Credit/Financial	Yes - Published #	31,000

In the email sent to about 31,000 customers affected by its data breach, E*Trade warned that in late 2013, some of their personal information had been compromised by attackers, The Washington Post reports. But there is "no evidence that any sensitive customer account information, including passwords, Social Security numbers or financial information was compromised," the e-mail reportedly said. It added that there had been "no reports of financial fraud or loss resulting from this incident," and offered affected individuals one year of prepaid identity theft monitoring.

Attribution 1 Publication: bankinfosecurity.com Author:
Article Title: E*Trade, Dow Jones Issue Breach Alerts
Article URL: http://www.bankinfosecurity.com/etrade-dow-jones-issue-breach-alerts-a-8586

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151013-05	Office of Peggy E. Olson, CPA	MT	10/9/2015	Electronic	Business	Yes - Published #	Unknown

On September 2, 2015, a virus infected my computer and an unauthorized individual may have gained access to my computer for a limited period of time- less than one hour. While your information was stored in a file on my computer and I think it highly unlikely that the unauthorized individual accessed your information, I wanted to let you know about this event out of an abundance of caution. The file may have contained your name, address, and Social Security number.

Attribution 1 Publication: VT AG's office Author:
Article Title: Office of Peggy E. Olson, CPA
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Peggy%20Olson%20SBN.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151013-04	Peppermill Casinos, Inc.	NV	10/5/2015	Electronic	Business	Yes - Unknown #	Unknown

This security incident relates to the unauthorized and illegal acquisition, by criminal hackers, of certain credit and debit cards used at Peppermill's front desk. The criminal attack was limited to credit or debit transactions between October 12, 2014 and February 16, 2015, and we became aware of the existence, nature and extent of the security incident in late Apri12015. However, we delayed notification due to an ongoing investigation by law enforcement.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: Peppermill Casinos, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Peppermill%20Resort%20Spa%20Casino%20SBN%20t

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151013-03	CarePlus Health Plans	FL	10/11/2015	Paper Data	Medical/Healthcare	Yes - Published #	2,873

On September 18, 2015, CarePlus prepared a mailing of CarePlus Late Enrollment Penalty Premium Statements to patients. A machine was used to insert two premium statements into each envelope, but instead of inserting one statement, two were placed into each envelope by accident. The error resulted in 1,400 patients being sent statements intended for other patients.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: CarePlus Health Plans
Article URL: http://www.hipaajournal.com/careplus-discovers-privacy-breach-affecting-1400-8141/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151013-01	SSM Health Cancer Care	MO	10/9/2015	Paper Data	Medical/Healthcare	Yes - Published #	643

SSM Health Cancer Care MO Healthcare Provider 643 10/09/2015Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: SSM Health Cancer 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
ITRC20151009-06	MARTA	GA	10/8/2015	Paper Data	Business	Yes - Published #	785

MARTA accidentally mailed the personal information of 785 employees to incorrect addresses due to an “equipment malfunction,” the transportation agency reported Thursday. On June 8, during enrollment for critical care insurance for the roughly 785 MARTA employees, a mechanical malfunction occurred during the mail merge, which resulted in personal information -- such as date of birth and Social Security numbers -- being mailed to the incorrect addressees.

Attribution 1 Publication: Atlanta Business Chronicle Author:
Article Title: Data breach at MARTA exposes 785 employees
Article URL: http://www.bizjournals.com/atlanta/news/2015/10/08/data-breach-at-marta-exposes-785-employees.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151009-05	Schlage Lock Company	IL	10/6/2015	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you that on September 23, 2015, a company laptop computer containing employees' personal information was stolen from an offsite location. Personal information that may be stored on the laptop includes your name, email address, mailing address, telephone numbers, date of birth, salary and social security number. We have reported the theft to local law enforcement.

Attribution 1 Publication: VT AG's office / scmagazine.com Author:
Article Title: Schlage Lock Company
Article URL: http://www.scmagazine.com/employee-data-on-stolen-schlage-lock-company-laptop/article/450058/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151009-04	NorthShore Supply (Samela)	IL	8/24/2015	Electronic	Business	Yes - Unknown #	Unknown

On August 24, 2015, NorthShore Care Supply learned of a possible security incident involving its online ordering website. We immediately engaged independent IT forensic experts to assist with our investigation. While the investigation is still ongoing, it appears that your credit and debit card data may have been compromised if you made an online purchase between June 7, 2015 and August 24, 2015. The information potentially exposed includes your name, address, card number, verification code, and/or the card’s expiration date.

Attribution 1 Publication: CA AG's office / VT AG's office Author:
Article Title: NorthShore Supply
Article URL: https://oag.ca.gov/system/files/Samela%20dba%20NorthShore%20Supply%20notice%20only_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151009-03	glamglowmud.com (GlamGlow)	CA	5/20/2015	Electronic	Business	Yes - Unknown #	Unknown

We recently became aware that an unauthorized party accessed the glamglowmud.com website and acquired certain personal information of some of our customers.Based on the investigation, we believe the incident occurred between September 19 and September 21, 2014 and May 12 and May 15, 2015. The affected information may have included names; addresses; telephone numbers; payment card numbers, expiration dates and security codes; email addresses; and GlamGlow account passwords.

Attribution 1 Publication: CA AG's office Author:
Article Title: glamglowmud.com (GlamGlow)
Article URL: https://oag.ca.gov/system/files/Mail%20Notification%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151009-02	Vacaville Housing Authority	CA	10/9/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

On Monday, August 24, 2015, a VHA employee accidentally sent an email with a file that had your name and social security number to one person. The person who received the email was not authorized to view the information it contained, but she contacted us right away on August 25, 2015, to let us know what had happened. That person told the VHA that she deleted the email from her email inbox. The VHA immediately reported this incident to local police. The police spoke with the person and they made sure the email from the VHA was permanently deleted from her email inbox. The VHA is not aware of anyone using your personal information without your permission because of
this incident.

Attribution 1 Publication: CA AG's office Author:
Article Title: Vacaville Housing Authority
Article URL: https://oag.ca.gov/system/files/Vacaville%20Housing%20Authority%20-%20Notice%20of%20Data%20Event_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151009-01	Dow Jones & Co.	NY	10/9/2015	Electronic	Banking/Credit/Financial	Yes - Published #	3,500

"As part of the investigation to date, we also determined that payment card and contact information for fewer than 3,500 individuals could have been accessed, although we have discovered no direct evidence that information was stolen. We are sending those individuals a letter in the mail with more information about the support we are offering. If you do not receive such a letter, we have no indication that your financial information was involved," the letter states.

Attribution 1 Publication: cso.com / VT AG's office / NH AG's offic Author:
Article Title: Dow Jones & Co. discloses breach, incident likely related to Scottrade
Article URL: http://www.csoonline.com/article/2991378/data-breach/dow-jones-and-co-discloses-breach-incident-likely-related-to-s

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151007-01	Office of Daniel A. Sheldon	FL	9/16/2015	Electronic	Medical/Healthcare	Yes - Published #	2,075

On May 18, 2013, OCR received an anonymous complaint alleging that the protected health information (PHI) of the patients of the covered entity (CE), Dr. Daniel Sheldon, M.D., P.A., was accessible on the internet via Google. OCR confirmed the allegations when it identified web search results containing private medical records from a website associated with the practice. Following an investigation by OCR, the practice submitted a breach notification to HHS on September 16, 2015, in which it reported that the PHI of approximately 2,075 patients was potentially viewable online, including addresses, dates of birth, names, and clinical information.

Attribution 1 Publication: databreaches.net / OCR Author:
Article Title: Office of Daniel A. Sheldon
Article URL: http://www.databreaches.net/oh-so-thats-what-happened-sunday-edition/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151006-04	Department of Veterans Affairs - Palo Alto	CA	9/28/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

An inspector general's report revealed that Palo Alto's Department of Veterans Affairs facility provided patient information to a private IT company whose employees had not been cleared through background checks. The Sept. 28 report was instituted after a complaint by House Committee on Veterans' Affairs alleged that the VA Palo Alto Health Care System's informatics chief had entered into an illegal agreement with a healthcare tech company, Kyron, for sharing patient information.

Attribution 1 Publication: federaltimes.com Author:
Article Title: OIG: Palo Alto VA gave patient info to IT company
Article URL: http://www.federaltimes.com/story/government/it/2015/09/28/oig-palo-alto-va-gave-patient-info-company/72991040/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151006-03	Sunquest Information Systems	AZ	9/24/2015	Electronic	Medical/Healthcare	Yes - Published #	2,100

Sunquest Information Systems AZ Business Associate 2100 09/24/2015 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Sunquest Information 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
ITRC20151006-02	Kindred Nursing Centers West, LLC	CA	9/25/2015	Electronic	Medical/Healthcare	Yes - Published #	1,125

Kindred Nursing Centers West, L.L.C. CA Healthcare Provider 1125 09/25/2015 Theft Desktop Computer

Attribution 1 Publication: hhs.gov Author:
Article Title: Kindred Nursing Centers West, 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
ITRC20151006-01	Streets of New York	AZ	9/30/2015	Electronic	Business	Yes - Published #	250

We recently learned that the section of our online store at www.streetsofnewyork.com that processes gift card orders was subject to an online attack, and as a result, approximately 250 credit card numbers used for gift card purchases made since late 2009 and certain other customer information may have been accessed by unauthorized parties.

Attribution 1 Publication: VT AG's office Author:
Article Title: Streets of New York
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Streets%20of%20New%20York%20SBN%20to%20Cons

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151005-03	Skin and Cancer Center of Arizona	AZ	9/21/2015	Paper Data	Medical/Healthcare	Yes - Published #	3,311

Skin and Cancer Center of Arizona AZ Healthcare Provider 3311 09/21/2015 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Skin and Cancer Center of Arizona
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
ITRC20151005-02	Schwab Retirement Plan Services	CA	8/25/2015	Electronic	Banking/Credit/Financial	Yes - Published #	9,400

On August 25th, a spreadsheet containing your Social Security number, name, address, date of birth, date of termination (if applicable), employment status, division code, marital status and account balance was accidentally emailed to a participant in another retirement plan serviced by SRPS. That person immediately informed their plan sponsor, who in turn contacted SRPS. T

Attribution 1 Publication: CA AG's office Author:
Article Title: Schwab Retirement Plan Services
Article URL: https://oag.ca.gov/system/files/Participant%20Incident%20Notification%20Template%2010_1_15_0.pdf?

Attribution 2 Publication: scmagazine.com Author:
Article Title: Email incident affects 9,400 Schwab Retirement Plan Services participants
Article URL: http://www.scmagazine.com/email-incident-affects-9400-schwab-retirement-plan-services-participants/article/444729/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151005-01	Ferndale Housing Commission	MI	10/4/2015	Paper Data	Government/Military	Yes - Unknown #	Unknown

Illegal dumping in Detroit is not uncommon - but one case in Brightmoor is especially alarming. It was bad enough to have to look at the mess, but what Graham Emerson found recently was enough to send the grizzled Detroiter over the top. A moderate pile of junk included personal documents from the Social Security Administration and the Ferndale Housing Commission.

Attribution 1 Publication: databreaches.net / Fox2Detroit Author:
Article Title: Man wants to return personal docs found in illegal dumping
Article URL: http://www.databreaches.net/mi-man-wants-to-return-personal-docs-found-in-illegal-dumping/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151002-06	Scottrade	IL	9/25/2015	Electronic	Banking/Credit/Financial	Yes - Published #	812

WSC inadvertently mailed 1258 of these forms using addresses that Scottrade clients had provided for the 2012 and/or 2013 tax years, and which had not been updated to reflect changes of address. As a result these mailings were sent to old and outdated addresses. 428 of those have now been returned to our offices as undeliverable, leaving 812 with unknown outcomes. Those 1099 forms contained the client's name, address, eight-digit Scottrade account number and the last four digits of their Social Security Number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Scottrade
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/scottrade-financial-20150925.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151002-05	M&R Strategic Services, Inc.	DC	9/23/2015	Electronic	Business	Yes - Unknown #	Unknown

On August 10, 2015, M+R determined an unknown actor accessed without authorization its finance department email account and sent phishing emails to certain individuals and businesses affiliated with M+R. M+R immediately changed the credentials used to access the email account, enabled two-factor authentication, and communicated with certain recipients of the phishing email to encourage steps be taken to protect against unauthorized access to the recipients' information and systems.

Attribution 1 Publication: NH AG's office Author:
Article Title: M&R Strategic Services, Inc.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/m-r-strategic-svcs-20150923.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151002-04	American Bankers Association	DC	10/1/2015	Electronic	Business	Yes - Unknown #	Unknown

ABA has learned that email addresses and passwords used to make purchases or register for events through aba.com's Shopping Cart have been compromised. Though we are not aware of any fraudulent activity associated with this, we are taking the breach seriously and have launched an immediate investigation.

Attribution 1 Publication: ABA website / CA AG's office Author:
Article Title: ABA Shopping Cart Data Breach
Article URL: http://www.aba.com/About/Pages/Alert.aspx

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151002-03	Sentara Heart Hospital	VA	10/2/2015	Electronic	Medical/Healthcare	Yes - Published #	1,040

The theft occurred over the weekend of August 14 in a procedure area normally restricted to staff and patients. We believe these small portable hard drives were stolen for whatever street value they may have, and not for purposes of identity theft or fraud. The identifying information is so limited it does not facilitate fraud. The information on the drives is purely clinical. Updated procedures are in place for the secure storage of these devices. We sincerely regret any concern or inconvenience the theft of these devices may cause our patients.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: 1,040 Sentara Heart Hospital patients notified of HIPAA breach
Article URL: http://www.databreaches.net/1040-sentara-heart-hospital-patients-notified-of-hipaa-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151002-02	Scottrade	IL	10/2/2015	Electronic	Banking/Credit/Financial	Yes - Published #	4,600,000

St. Louis-based Scottrade said it recently heard from federal law enforcement officials about crimes involving the theft of information from Scottrade and other financial services companies. All client passwords remained encrypted at all times and we have not seen any indication of fraudulent activity as a result of this incident." The notice said that although Social Security numbers, email addresses and other sensitive data were contained in the system accessed, "it appears that contact information was the focus of the incident." The company said the unauthorized access appears to have occurred over a period between late 2013 and early 2014.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Scottrade Breach Hits 4.6 Million Customers
Article URL: http://krebsonsecurity.com/2015/10/scottrade-breach-hits-4-6-million-customers/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151002-01	Heartland Health Clinic	VA	9/21/2015	Electronic	Medical/Healthcare	Yes - Published #	3,650

Heartland Health Clinic VA Healthcare Provider 3650 09/21/2015 Hacking/IT Incident Desktop Computer, Electronic Medical Record, Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Heartland Health Clinic
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
ITRC20151001-01	T-Mobile / Experian	WA	10/1/2015	Electronic	Business	Yes - Published #	15,000,000

On September 15, 2015, we discovered that an unauthorized party accessed certain Experian servers. We immediately began to investigate the incident and to implement additional security measures. On September 21, 2015, we notified T-Mobile USA, Inc. that information Experian maintains on their behalf to perform credit checks had been downloaded by the unauthorized party. Information you provided when you applied for an account at Tmobile likely was acquired. That information includes your name, address, social security number, date of birth, identification number (such as driver's license, military ID, or passport number) and additional information used in T-Mobile's own credit assessment. No payment card or banking information was obtained.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Experian Breach Affects 15 Million Consumers
Article URL: http://krebsonsecurity.com/2015/10/experian-breach-affects-15-million-consumers/

Attribution 2 Publication: CA AG's office Author:
Article Title: T-Mobile / Experian
Article URL: https://oag.ca.gov/system/files/2015-10-01%20Multi-state%20notification%20letter%20-%20Experian%20incident%20-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-13	Pediatric Gastroenterology, Hepatology & Nutrition of	FL	8/24/2015	Paper Data	Medical/Healthcare	Yes - Published #	13,000

While we do not believe our patients have been harmed in any way, we have learned that certain patients' personal information, consisting of some of the following: name, social security number, account number, patient ID and date of birth, may have been compromised due to a recent theft at the Practice.

Attribution 1 Publication: tummydoctors.com Author:
Article Title: Pediatric Gastroenterology, Hepatology & Nutrition of Florida
Article URL: http://www.tummydoctors.com/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-12	North Oldham High School	KY	9/25/2015	Electronic	Educational	Yes - Published #	2,800

North Oldham High School is alerting 2,800 current and former students that a data breach earlier this month could have exposed their names, social security numbers and other personal information.

Attribution 1 Publication: databreaches.net Author:
Article Title: North Oldham High School student data potentially compromised after employee falls for phishing attempt
Article URL: http://www.databreaches.net/ky-north-oldham-high-school-student-data-potentially-compromised-after-employee-falls

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-11	U.S. Army Fee Assistance Program	DC	9/25/2015	Electronic	Government/Military	Yes - Published #	8,000

The families' medical histories, social security numbers, home addresses and child daycare information were made vulnerable. Unauthorized people or contractors have viewed the private information of at least 82 of those families, according to the federal General Services Administration, the agency that suffered the breached. The agency's inspector general says as many as 8,000 of the 9,000 Army families that use the program may have had their information compromised.

Attribution 1 Publication: nbcwashington.com Author:
Article Title: U.S. Army Fee Assistance Program
Article URL: http://www.nbcwashington.com/investigations/Security-Breaches-Expose-Private-Information-of-Military-Families-329

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-10	Big Blue Bus	CA	9/27/2015	Electronic	Business	Yes - Unknown #	Unknown

"On September 18, NextBus detected suspicious activity from an agency account and its IT experts worked quickly to minimize the issue. An unauthorized individual may have gained access to a database containing some account information of our NextBus agency customers and the riders that use NextBus services," said a BBB alert.

Attribution 1 Publication: Santa Monica Daily Press Author:
Article Title: Data breach involves Big Blue Bus customers
Article URL: http://smdp.com/data-breach-involves-big-blue-bus-customers/151000

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-09	Barrington Orthopedic Specials	IL	9/28/2015	Electronic	Medical/Healthcare	Yes - Published #	1,009

Barrington Orthopedic Specialists, Ltd. takes patient privacy very seriously, and it is important to us that you are made fully aware of a potential privacy issue. We have learned that some patient's personal information may have been compromised.

Attribution 1 Publication: databreaches.net / hipaajournal.com Author:
Article Title: Barrington Orthopedic Specialists, Ltd notifies patients after theft of equipment
Article URL: http://www.databreaches.net/barrington-orthopedic-specialists-ltd-notifies-patients-after-theft-of-equipment/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-08	Hilton Worldwide	VA	9/29/2015	Electronic	Business	Yes - Unknown #	Unknown

Multiple sources in the banking industry say they have traced a pattern of credit card fraud that suggests hackers have compromised point-of-sale registers in gift shops and restaurants at a large number of Hilton Hotel and franchise properties across the United States. Hilton says it is investigating the claims.

Attribution 1 Publication: bankinfosecurity.com Author:
Article Title: Hilton Hotels: We Were Breached
Article URL: http://www.bankinfosecurity.com/hilton-hotels-we-were-breached-a-8703?rf=2015-11-25-eb&mkt_tok=3RkMMJWWfF9

Attribution 2 Publication: krebsonsecurity / CA AG's office Author:
Article Title: Banks: Card Breach at Hilton Hotel Properties
Article URL: http://krebsonsecurity.com/2015/09/banks-card-breach-at-hilton-hotel-properties/

Attribution 3 Publication: 11/30/2015 Author:
Article Title: Hilton confirms credit card breach at property stores and restaurants
Article URL: http://www.foxnews.com/travel/2015/11/30/hilton-confirms-credit-card-breach-at-property-stores-and-restaurants/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-07	Insurance Data Services (IDS) /Claystone Clinical	WY	9/27/2015	Electronic	Medical/Healthcare	Yes - Published #	2,900

Insurance Data Services (IDS), a Wyoming-based medical billing company, has started to send breach notification letters to patients of one of its HIPAA-covered clients, Claystone Clinical Associates, to advise them of the potential exposure of some of their Protected Health Information (PHI). IDS had contracted a West Michigan based Delivery Service to deliver client mailings; however the vehicle used by the courier company was stolen on September 15. The vehicle theft occurred at Zondervan Publishing in Kentwood, MI.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Car Theft Results in Exposure of PHI of 2900 Individuals
Article URL: http://www.hipaajournal.com/car-theft-results-in-exposure-of-phi-of-2900-individuals-8117/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-06	Horizon Blue Cross Blue Shield of New Jersey	NJ	9/28/2015	Electronic	Medical/Healthcare	Yes - Published #	1,173

Criminals posing as doctors are behind a recent Horizon Blue Cross Blue Shield of New Jersey data breach. The bogus physicians obtained Horizon BCBSNJ member ID numbers of patients and other sensitive Protected Health Information only available to legitimate healthcare professionals. The information was stolen in order for the criminals to file false insurance claims in the names of the victims. Fraudulent activity was first uncovered on July 30, 2015 and approximately 1,100 individuals are understood to have been affected by the security breach.

Attribution 1 Publication: hipaajournal.com / Scmagazine.com / h Author:
Article Title: Bogus Doctors Behind Horizon Blue Cross Blue Shield of New Jersey Data Breach
Article URL: http://www.hipaajournal.com/bogus-doctors-behind-horizon-blue-cross-blue-shield-of-new-jersey-data-breach-8118/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-05	Bed Bath & Beyond	NJ	9/22/2015	Electronic	Business	Yes - Unknown #	Unknown

We have conducted an internal investigation and determined this potential compromise was an isolated incident that occurred in one specific store with one specific cashier during this specific time period. That cashier has since been removed from Bed Bath & Beyond and we are taking the necessary legal action. We take the confidentiality of our customers' [REDACTED] information very seriously and we want to ensure our customers are informed in order to detect and prevent potential unauthorized charges on their cards.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: Bed Bath & Beyond
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Bed%20Bath%20and%20Beyond%20SBN%20to%20Co

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-04	padlocks4less.com / Frank J. Martin Company	WA	9/22/2015	Electronic	Business	Yes - Unknown #	Unknown

We were recently notified by the Federal Bureau of Investigation (the FBI) that credit card data used on the website www.padlocks4less.com may have been accessed without authorization. The information included your name, address, phone number, email address and payment card data. The information did not include your Social Security number, nor did it include debit or credit card PINs, bank account numbers or any other personal information. We do not know how the information was accessed, nor do we know who accessed it, but the FBI believes it occurred between June 3 and August 26, 2015.

Attribution 1 Publication: VT AG's office / scmagazine.com Author:
Article Title: padlocks4less.com / Frank J. Martin Company
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/padlocks4less%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-03	Trump Hotel Collection	NV	6/2/2015	Electronic	Business	Yes - Unknown #	Unknown

While the independent forensic investigator did not find evidence that information was taken from the Hotel's systems, it appears that there may have been unauthorized malware access to payment card information as it was inputted into the payment card systems. Payment card data (including payment card account number, card expiration date, security code, and cardholder name) of individuals who used a payment card at the Hotel between May 19, 2014, and June 2, 2015, may have been affected.

Attribution 1 Publication: CA AG's office Author:
Article Title: Trump Hotel Collection
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-02	Silverberg Surgical and Medical Group	CA	8/28/2015	Electronic	Medical/Healthcare	Yes - Published #	857

We are sending this notification to you because we recently discovered a security breach involving some of your personal health information. Based on our investigation, on September 10, 2013 a document scanning device inadvertently exposed some patient health records to the Internet. The records that were accessible included patient names, addresses, dates of birth and admission, telephone and fax numbers, e-mail addresses, medical information, medical record numbers, health plan data and beneficiary numbers, and, in some cases Social Security numbers, State License numbers and full face photographic images.

Attribution 1 Publication: CA AG's office / hipaajournal.com / hhs. Author:
Article Title: Silverberg Surgical and Medical Group
Article URL: http://www.hipaajournal.com/document-scanner-error-exposes-phi-of-silverberg-surgical-and-medical-group-patients-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150929-01	Kindred Transitional Care and Rehabilitation - Lawton	KY	9/22/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On August 31, 2015, we learned that an office computer had been stolen from a locked office within the facility. We believe that the theft occurred between August 28 and August 31. On September 1, we learned one or more files containing certain information about you were stored on the computer. The information included your name and one or more of the following: admission and discharge dates, facility name, Kindred-issued patient number, and certain accounting-related information such as copayment or days of Medicare use.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Kindred Transitional Care and Rehabilitation - Lawton
Article URL: https://oag.ca.gov/system/files/Lawton%20notice%20-%20deidentified_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-13	Blue Cross Blue Shield - North Carolina #2	NC	9/11/2015	Paper Data	Medical/Healthcare	Yes - Published #	1,530

A second error was discovered by BCBSNC a few days later on August 24. Plan members had been sent information intended for other subscribers. In this incident, payment amounts, payment ID numbers, health insurance marketplace identification numbers, details of health plans purchased, and their effective dates were disclosed. An error was made on a spreadsheet which resulted in the wrong information being sent to the printers. Affected individuals are not believed to face an increased risk of suffering insurance fraud, although HIPAA Rules required notifications to be sent to patients nonetheless to alert them to the privacy breach.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Two Blue Cross and Blue Shield of North Carolina Printing Errors Discovered
Article URL: http://www.hipaajournal.com/printing-errors-cause-3-health-plan-data-breaches-8135/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-12	Blue Cross Blue Shield - North Carolina #1	NC	9/11/2015	Paper Data	Medical/Healthcare	Yes - Published #	807

The first error was brought to the attention of BCBSNC on August 14 after complaints were received about a recent mailing sent to its subscribers.
A printing error saw members' billing information printed on the reverse side of other plan members' invoices. No personal financial information was disclosed; although some plan members did have their names, addresses, coverage dates, premium amounts, and internal BCBSNC account numbers disclosed. The incident did not result in the unauthorized disclosure of BCBSNC member identification numbers according to the breach notice.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Two Blue Cross and Blue Shield of North Carolina Printing Errors Discovered
Article URL: http://www.hipaajournal.com/printing-errors-cause-3-health-plan-data-breaches-8135/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-11	ACE Surgical Supply Co.	MA	9/15/2015	Electronic	Business	Yes - Published #	4,300

I am writing on behalf of my client, ACE Surgical Supply Co., Inc. ("ACE"), to inform you of an information security incident that occurred, which possibly involved thirteen (13) New Hampshire residents. During a routine review of its server performance data, an ACE technician discovered a performance issue which prompted ACE to conduct a more thorough review of the system. After further review, they discovered suspicious files that prompted them to investigate further.
ACE hired RSA, the Security Division of EMC, to assist in the investigation. From RSA's findings, it appears that credit card information and/or account passwords of a small number of customers may have been compromised.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: ACE Surgical Supply Co.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/ace-surgicalsupply-20150915.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-10	Costco Photo Center / PNI Digital Media	WA	9/18/2015	Electronic	Business	Yes - Unknown #	Unknown

Costco is telling customers they can start ordering photos online again, seven weeks after a security breach at a third-party hosting company forced it and several other photo ordering sites to go down in mid-July. The Issaquah, Wash.-based big-box retailer says customer photos weren't compromised in the hack, but the company warns in an FAQ, "At this point, we believe that the credit card information of a small percentage of Costco members was captured." Costco's FAQ continues, "Users placing orders for warehouse pick-up may have had their username and password compromised. Users placing mail orders for home delivery may have had their credit card information, mailing address, as well as username and password compromised."

Attribution 1
Publication: geekwire.com / VT AG's office Author:
Article Title: Costco Photo Center finally back online after security breach forces seven-week outage
Article URL: http://www.geekwire.com/2015/costco-photo-center-finally-back-online-after-security-breach-forces-seven-week-outag

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-09	YapStone (VacationRentPayment)	CA	9/11/2015	Electronic	Business	Yes - Unknown #	Unknown

YapStone (which you may know as VacationRentPayment), a provider of payment services is writing to inform you that certain personal information you provided on your VacationRent Payments application that was stored by YapS tone may have been accessible by unauthorized persons via a YapStone URL between approximately July 15,2014 and August 5, 2015. Unfortunately, due to this application being available, your email, Social Security number, driver's license, date of birth, and bank account were potentially exposed. Please review the enclosed F AQ for additional information.

Attribution 1
Publication: VT AG's office / MD AG's office Author:
Article Title: YapStone (VacationRentPayment)
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Yapstone%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-08	TD Bank	NJ	9/16/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently learned that one of our employees obtained and inappropriately used confidential customer information and provided it to an unauthorized party not associated with TD Bank. The personal information they obtained may have included name, address, and account number of the primary account holders and potentially their secondary signers and/or beneficiaries. This is an isolated incident that is being addressed through an internal investigation by our corporate security team and we have contacted local law enforcement.

Attribution 1
Publication: databreaches.net / NH AG's office Author:
Article Title: Yet another insider breach at TD Bank. Paging regulators to Aisle 4…?
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/td-bank-20150904.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-07	Hackers breach Commack High School computer	NY	9/18/2015	Electronic	Educational	Yes - Unknown #	Unknown

The District has become aware that the student management system at the High School was accessed by an unauthorized person. At this time, there is no evidence that the individual downloaded any specific student data. However, we thought it was important to make parents aware of the potential release of student data. At this time, we believe this breach only applies to a very limited number of high school student records. Types of information that may have been viewed include: student ID numbers, name, address, contact information, and student schedules. Social security numbers are NOT in the student management system.

Attribution 1
Publication: databreaches.net / school website Author:
Article Title: Hackers breach Commack High School computer system, district officials say
Article URL: http://www.commack.k12.ny.us/communitynews/announce-studentdata.asp

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-06	Central New Mexico Community College	NM	9/18/2015	Electronic	Educational	Yes - Published #	3,000

Thousands of Central New Mexico Community College students could be at risk of having their personnel information compromised. The college said someone from the health center reported in July that a thumb drive with students' birth dates and Social Security numbers was missing. The college does not know what happened to it.

Attribution 1 Publication: koat.com / databreaches.net Author: Mike Springer
Article Title: Mike Springer By Mike Springer
Article URL: http://www.koat.com/news/cnm-student-information-possibly-compromised/35340518

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-05	Lee Memorial Health System	FL	9/7/2015	Paper Data	Medical/Healthcare	Yes - Published #	1,508

Lee Memorial Health System FL Healthcare Provider 1508 09/07/2015 Unauthorized Access/Disclosure Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-04	Minneapolis Clinic of Neurology	MN	8/31/2015	Electronic	Medical/Healthcare	Yes - Published #	1,450

Minneapolis Clinic of Neurology, Ltd. MN Healthcare Provider 1450 08/31/2015 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Minneapolis Clinic of Neurology
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
ITRC20150922-03	Affinity Health Plan, Inc.	NY	9/14/2015	Paper Data	Medical/Healthcare	Yes - Published #	496

On Friday, August 14, 2015, Affinity discovered that a double-sided (English/Spanish or English/Chinese language) renewal letter that was mailed to heads of household on August 4, 2015, had shifted by one page during print production. This shift caused an error that resulted in some heads of household receiving letters with a different head of household's name, address and children's name(s) and unique Affinity member identification number(s) on the back of the letter. (HHS = 721)

Attribution 1 Publication: databreaches.net / hhs.gov Author: 10/6/2015
Article Title: Affinity Health Plan notifies members of PHI breach
Article URL: http://www.databreaches.net/affinity-health-plan-notifies-members-of-phi-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-02	Outback / T-Bird Restaurant Group	FL	8/7/2015	Electronic	Business	Yes - Unknown #	Unknown

Computer equipment, including the restaurant's point of sale computer terminal and back office computer, was stolen and the thief or thieves attempted to steal the restaurant's safe. The point of sale computer contains current and archived employee time sheet information, including files that contain your name and social security number. The time sheet program does not store your address, driver's license number, credit card number, or personal medical information and therefore we have no reason to believe that information was included in the theft. Employee information is not stored on the back office computer.

Attribution 1 Publication: CA AG's office / Scmagazine.com Author:
Article Title: Outback / T-Bird Restaurant Group
Article URL: https://oag.ca.gov/system/files/Outback%20Notice_final_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150922-01	Molina Healthcare / CVS	CA	9/17/2015	Electronic	Medical/Healthcare	Yes - Published #	54,203

This is to let you know that CVS, Molina Healthcare's Over-the-Counter (OTC) benefits vendor, told us on 7/20/15 about a breach of your protected health information (PHI). On or about 3/26/15, a former CVS employee took PHI from CVS' computers and sent it to his personal computer. CVS believes he did this to fraudulently obtain OTC products from CVS. Upon learning of this incident, CVS took prompt action to investigate this issue. No fraudulent use of your PHI has been found. The PHI involved in the breach is as follows: Full Name; CVS ID; CVS ExtraCare Health Card Number; Member ID; Rx Plan Number; Rx Plan State; Start Date; and End Date.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
Article Title: Molina Healthcare / CVS
Article URL: https://oag.ca.gov/system/files/SAMPLE%20Final%20Member%20Breach%20Notification%20DSNP%20CA%20WA%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150915-07	**Charlotte-Mecklenburg Schools notifies 7,600 job**	NC	9/15/2015	Electronic	Educational	Yes - Published #	**7,600**

Charlotte-Mecklenburg Schools has notified about 7,600 job applicants that their personal information, including Social Security numbers, was shared with an outside contractor without their consent.

Attribution 1 Publication: databreaches.net / The Charlotte Obser Author:
Article Title: CMS alerts 7,600 job applicants to personal data breach
Article URL: http://www.charlotteobserver.com/news/local/education/article35300451.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150915-06	**Systema Software**	CA	9/15/2015	Electronic	Medical/Healthcare	Yes - Published #	**1,500,000**

According to a source who contacted DataBreaches.net, as part of research on data leaks, the self-described “technology enthusiast” (“TE”) downloaded some random data from a publicly available subdomain on Amazon Web Services (AWS). Inspection of the files revealed many GB of SQL database backups with “names, social security numbers, addresses, dates of birth, phone numbers, as well as various financial and medical injury data.”

Attribution 1 Publication: CA AG's office Author:
Article Title: George Hills Company
Article URL: https://oag.ca.gov/ecrime/databreach/reports/sb24-59212

Attribution 2 Publication: hipaajournal.com Author:
Article Title: SYSTEMA SOFTWARE DATA BREACH: 1.5M+ MEDICAL RECORDS ACCESSIBLE VIA AWS
Article URL: http://www.hipaajournal.com/systema-software-data-breach-1-5-m-records-aws-8110/

Attribution 3 Publication: databreaches.net / ihealthbeat.org Author:
Article Title: Oops! Error by Systema Software exposes millions of records with insurance claims data and internal notes (Update2)
Article URL: http://www.databreaches.net/oops-error-by-systema-software-exposes-millions-of-records-with-insurance-claims-data

Attribution 4 Publication: databreaches.net Author:
Article Title: Error by Systema Software exposes millions of records with insurance claims data and internal notes
Article URL: http://www.databreaches.net/oops-error-by-systema-software-exposes-millions-of-records-with-insurance-claims-data

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150915-05	**LSU Health New Orleans School of Medicine**	LA	9/15/2015	Electronic	Medical/Healthcare	Yes - Published #	**14,500**

A laptop stolen from a member of the faculty of LSU Health New Orleans School of Medicine has potentially exposed the protected health information of approximately 5,000 minor patients primarily living in Louisiana and Mississippi. Dr. Christopher Roth, Assistant Professor of Urology, reported that his university-issued laptop was stolen from his car sometime between the evening hours of July 16 and the early morning hours of July 17, 2015. The car was parked in front of his home. The information on the laptop included names, dates of birth, dates of treatment, descriptions of patients’ conditions, treatments, and outcomes, lab test results, radiological and ultrasound images, medical record numbers, and diagnosis and treatment information. No Social Security numbers, credit card, bank account information or other financial data were stored on the laptop. (14,500 = hhs.gov)

Attribution 1 Publication: databreaches.net / hipaa journal /hhs.go Author:
Article Title: Laptop with 5,000 minors’ protected health info stolen from doctor’s unattended car
Article URL: http://www.databreaches.net/la-laptop-with-5000-minors-protected-health-info-stolen-from-doctors-unattended-car/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150915-04	Vermont Health Connect	VT	9/11/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A Vermont Health Connect staff member reported that on 9/15 they inadvertently emailed copies of your eligibility notices, invoices, and screen shots of your account information to the wrong customer. The attachment in the email contained your name, your address, your email address, your Social Security Number, your reported income, your health insurance enrollment, your health insurance premium amounts and your advanced premium tax credits.

Attribution 1 Publication: VT AG's office Author:
Article Title: Vermont Health Connect
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Vermont%20Health%20Connect%20SBN%20to%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150915-03	Glidewell Laboratories / Dental Ceramics, Inc. /	OH	7/31/2015	Electronic	Business	Yes - Unknown #	Unknown

Glidewell recently learned that an unauthorized individual may have taken certain documents and data maintained and/or owned by Glidewell, without Glidewell's authorization. Based upon a forensic investigation conducted by outside datasecurity experts retained by Glidewell to assist in this matter, we believe that certain employee-personnel data may have been taken along with other Glidewell proprietary information, including your name, address, social security number, and financial account information relating to your direct deposit account.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: Glidewell Laboratories / Dental Ceramics, Inc. / James R. Glidewell
Article URL: https://oag.ca.gov/system/files/Glidewell_Proof%20Copy_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150915-02	Sutter Health / Sutter Medical Foundation	CA	9/11/2015	Electronic	Medical/Healthcare	Yes - Published #	2,302

Sacramento, Calif.-based Sutter Health is notifying patients of a potential data breach after a former employee emailed electronic versions of billing documents to a personal account without authorization. The incident compromises the information of 2,582 patients. (2302 - hhs.gov)

Attribution 1 Publication: CA AG's office / beckershospitalreview.c Author:
Article Title: Sutter Health notifies 2,500 of breach after employee improperly emails billing documents
Article URL: http://www.beckershospitalreview.com/healthcare-information-technology/sutter-health-notifies-2-500-of-breach-after-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150915-01	Children's Hospital Medical Center of Akron	OH	8/26/2015	Electronic	Medical/Healthcare	Yes - Published #	7,664

The covered entity (CE) reported that a hard drive was missing that contained approximately 1,800 hours of voice recordings that were communications between dispatchers and medical staff prior to or during medical transport between September 18, 2014, and June 3, 2015.

Attribution 1 Publication: hhs.gov Author:
Article Title: Children's Hospital Medical Center of Akron
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
ITRC20150911-03	Pentagon Food Court	VA	9/9/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

"Within the past week, the Pentagon Force Protection Agency has received numerous reports of fraudulent use of credit cards belonging to Pentagon personnel. These individuals had fraudulent charges to their account soon after they had legitimate transactions at the Pentagon," according to a copy of the notice to employees obtained by the Washington Examiner.

Attribution 1 Publication: databreaches.net / washingtonexaminer. Author:
Article Title: Pentagon food court computers hacked, exposing employees' bank information
Article URL: http://www.washingtonexaminer.com/pentagon-food-court-computers-hacked-exposing-employees-bank-information/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150911-02	Oakland Family Services	MI	9/11/2015	Electronic	Medical/Healthcare	Yes - Published #	16,107

An unauthorized individual remotely gained access to the email account of an Oakland Family Services employee July 14, 2015 resulting in the potential viewing of protected health information (PHI). However, there was no infiltration of the electronic medical record databases, or any other agency email accounts or databases. The unauthorized access was discovered by Oakland Family Services that same day, when it was determined the employee's email account was fraudulently accessed as part of a phishing attempt. Phishing is an attempt to acquire sensitive information, such as usernames and passwords, utilizing emails that masquerade as those from a trustworthy entity.

Attribution 1 Publication: databreaches.net / HIPAA journal Author:
Article Title: Oakland Family Services security breached, 16K clients affected
Article URL: http://www.databreaches.net/mi-oakland-family-services-security-breached-16k-clients-affected/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150911-01	Excellus Blue Cross Blue Shield / Lifetime Healthcare	NY	9/10/2015	Electronic	Medical/Healthcare	Yes - Published #	10,000,000

Excellus revealed the breach on Wednesday, telling customers they would receive identity-monitoring services and that the FBI is investigating the crime. The records included Social Security numbers and other identifying information, as well as claims members made to pay for medical care.

Attribution 1 Publication: cnet.com / hhs.gov Author:
Article Title: Data breach exposes 10M health records from New York insurer
Article URL: http://www.cnet.com/news/data-breach-exposes-10m-health-records-from-new-york-insurer/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150908-05	Heritage Foundation	DC	9/2/2015	Electronic	Business	Yes - Unknown #	Unknown

We experienced a malicious, unauthorized data breach of six-year-old documents on an external server that appear to contain personal information of private donors, who we are notifying. We are unable to verify the authenticity of files circulated online.

Attribution 1 Publication: thehill.com Author:
Article Title: Heritage Foundation hit by hackers
Article URL: http://thehill.com/blogs/blog-briefing-room/news/252615-heritage-foundation-hit-by-hackers-report

Attribution 2 Publication: Heritage Foundation website Author:
Article Title: September 2, 2015
Article URL: http://www.heritage.org/research/reports/2015/09/heritage-foundation-statement-on-unauthorized-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150908-04	Viewpoint Construction Software	OR	8/28/2015	Electronic	Business	Yes - Published #	115

On July 15, 2015, Viewpoint learned that, on July 9, 2015, an unauthorized person gained access to Viewpoint's electronic payroll system and modified the direct deposit routing instructions for 115 employee records. Viewpoint later determined through a forensic investigation that the unauthorized person had used malware to obtain a Viewpoint manager's user-name and password to gain access to the payroll system. While in the system, the perpetrator may have had access to certain personal information, including employee names, addresses, Social Security numbers, salaries, email addresses and direct deposit information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Viewpoint Construction Software
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/viewpoint-20150828.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150908-03	We End Violence / California State Universitites	CA	9/4/2015	Electronic	Business	Yes - Published #	79,000

What Happened? OnAugust 24, 2015 we discovered a potential intrusion into ourwebsite server.We quickly moved to investigate this issue. In an abundance of caution, we took down the Agent of Change website on August 26, 2015. Third-party computer forensics experts were retained to assist with an investigation into the nature and scope of any intrusion. While the investigation is ongoing, it has been determined that there was unauthorized access to certain personal information relating to you, including your name, student ID number, email address (both the one provided by the school and any email provided by you upon registering), your Agent of Change username, your Agent of Change
password, gender identity, race, ethnicity, age, relationship status, sexual identity and the name of your college or university.

Attribution 1 Publication: CA AG's office / sbsun.com Author: Josh Dulaney
Article Title: We End Violence
Article URL: http://www.sbsun.com/social-affairs/20150908/csu-79k-students-had-data-breached-on-third-party-website

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150908-02	ReverbNation	NC	9/3/2015	Electronic	Business	Yes - Unknown #	Unknown

ReverbNation was recently contacted by law enforcement and alerted that an individual had illegally sought to gain unauthorized access to some of our customer's user data. In January 2014, an individual, who has since been identified and charged, illegally accessed a ReverbNation vendor's computer systems and ultimately gained unauthorized access to user information contained in a backup of our database. The information included in the database may have included your name, social security number, employer identification number, e-mail address, encrypted password, postal address, phone number, date of birth, and possibly other user information you may have provided to us.

Attribution 1 Publication: databreaches.net / scmagazine.com / C Author:
Article Title: ReverbNation notifies users of breach, recommends changing passwords
Article URL: http://www.databreaches.net/reverbnation-notifies-users-of-breach-recommends-changing-passwords/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150908-01	Hawaii First Federal Credit Union	HI	9/3/2015	Electronic	Banking/Credit/Financial	Yes - Published #	5,965

Hawaii First Federal Credit Union is notifying an undisclosed number of customers that an unauthorized individual may have gained access to an employee's email account, and could have accessed personal information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Hawaii First Federal Credit Union
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-257743.pdf

Attribution 2 Publication: scmagazine.com / MD AG's office Author:
Article Title: Hawaii credit union notifies customers of employee email breach
Article URL: http://www.scmagazine.com/hawaii-credit-union-notifies-customers-of-employee-email-breach/article/436785/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150904-01	Metropolitan Atlanta Rapid Transit	GA	8/27/2015	Paper Data	Medical/Healthcare	Yes - Published #	800

Metropolitan Atlanta Rapid Transit Authority GA Health Plan 800 08/27/2015 Unauthorized Access/DisclosurePaper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Metropolitan Atlanta Rapid Transit
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
ITRC20150903-02	Lancaster Cardiology Medical Group / Sunder	CA	8/24/2015	Electronic	Medical/Healthcare	Yes - Published #	1,200

Lancaster Cardiology Medical Group, and Sunder Heart Institute and Vascular Medical Clinic CA Healthcare Provider 1200 08/24/2015 Theft Desktop Computer, Laptop, Network Server, Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: Lancaster Cardiology Medical Group / Sunder Heart Institute an Vascular Medical Clinic
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
ITRC20150903-01	PT Northwest	OR	8/21/2015	Electronic	Medical/Healthcare	Yes - Published #	1,500

PT Northwest, LLC OR Healthcare Provider 1500 08/21/2015 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: PT Northwest
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
ITRC20150901-11	Santander Bank #4	NY	8/7/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On July 9, 2015, the Santander Bank Fraud Card Detection group discovered suspicious AIM withdrawals that occurred on July 8, 2015. Upon further investigation, it was determined that a magnetic stripe skimming device had been placed on the AIM vestibule door of our remote ATM located at 150-28 Union Square, Flushing, New York. After reviewing video surveillance footage, it was determined that the device had been placed on the AIM vestibule door on October 10, 2014 and removed October 15, 2014. The persona l information potentially compromised included the customer's name, ca rd number, card expiration date, card security code, and card PIN number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Santander Bank #4
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/santander-20150805.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-10	Santander Bank #3	MA	7/10/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On June 14, 2015, the Santander Bank Fraud Card Detection group discovered susp1c1ous ATM withdrawals that occurred that day. Upon further investigation, it was determined that a magnetic stripe skimming device had been placed on the ATM vestibule door of our remote ATM located at 65 Boston Street, Dorchester, MA. After reviewing video surveillance footage, it was determined that the device had been placed on the ATM vestibule door on June 10, 2015 and removed June 10, 2015. A device was again placed on and removed from the vestibule door on both June 11, 2015 and June 12, 2015. The personal information potentially compromised included the customer's name, card number, card expiration date, card security code, and card PIN number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Santander Bank
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/santander-bank-20150708.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-09	Santander Bank #2	MA	6/22/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On May 4, 2015, the Santander Bank Fraud Card Detection group discovered susp1oous ATM withdrawals that occurred on May 3, 2015. Upon further investigation, it was determined that a magnetic stripe skimming device had been placed on the ATM vestibule door of our branch located at 19 Pleasant Street, Woburn, MA. After reviewing the branch's video surveillance footage, it was determined that the device had been placed on the ATM vestibule door on May 1, 2015 and removed May 2, 2015. The personal information potentially compromised included the customer's name, card number, card expiration date, card security code, and card PIN number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Santander Bank
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/santander-bank-20150618.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-08	Michigan Catholic Conference	MI	8/31/2015	Electronic	Business	Yes - Unknown #	Unknown

The problem surfaced in late July, when IT staff for the Michigan Catholic Conference found a suspicious file deep within the organization's computer network. Work sites affected included Catholic churches, schools, hospitals, orphanages and diocesan offices. It is likely the attackers got away with employee names, Social Security numbers, dates of birth, addresses and monthly wage amounts.

Attribution 1 Publication: nextgov.com Author:
Article Title: Michigan Catholic Conference
Article URL: http://www.nextgov.com/cybersecurity/2015/08/hackers-breach-catholic-agencys-security-stalk-two-year-old-indiana-gi

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-07	BNY Mellon	NY	8/31/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Another bizarre incident occurred in the ongoing litigation between the sons of renowned East Hampton sculptor Norman Mercer and BNY Mellon (BNYM), which is administering his estate, when the bank improperly turned over personal and financial information about its other trust account beneficiaries residing in the New York Tri-state area.

Attribution 1 Publication: databreaches.net Author:
Article Title: BNY Mellon accused of leaking confidential client data
Article URL: http://www.databreaches.net/bny-mellon-accused-of-leaking-confidential-client-data/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-06	UCLA Health	CA	9/1/2015	Electronic	Medical/Healthcare	Yes - Published #	1,242

UCLA Health is sending notification letters to 1,242 individuals about the theft of a laptop computer containing patient names, medical record numbers, and health information used to help prepare patient treatment plans. No social security numbers, health plan ID numbers, credit card numbers, or other financial data were stored on the stolen lapto

Attribution 1 Publication: databreaches.net Author:
Article Title: UCLA Health notifying patients of stolen laptop containing personal health information; third breach report in as many months?
Article URL: http://www.databreaches.net/ucla-health-notifying-patients-of-stolen-laptop-containing-personal-health-information-th

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-05	Village Pizza & Pub	IL	9/1/2015	Electronic	Business	Yes - Unknown #	Unknown

On July 27, 2015, Village Pizza & Pub learned that the company that provides its point-of-sale payment card processing system, TransformPOS, had been the victim of a security incident. An unauthorized person used malware to gain access to Village Pizza's transaction information as it was being routed through the TransformPOS system.

Attribution 1 Publication: databreaches.net Author:
Article Title: Village Pizza & Pub notifies customers of data security breach at TransformPOS
Article URL: http://www.databreaches.net/il-village-pizza-pub-notifies-customers-of-data-security-breach-at-transformpos/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-04	Utah Food Bank	UT	8/31/2015	Electronic	Business	Yes - Published #	10,385

Utah Food Bank is notifying more than 10,000 individuals that their personal information – including payment card data – may have been exposed during a possible data security incident involving the donation webpage. What type of personal information? Names, addresses, email addresses, credit or debit card numbers, security codes and expiration dates. What happened? The personal information – including payment card data – may have been exposed during a possible data security incident involving the Utah Food Bank donation webpage.

Attribution 1 Publication: Scmagazine.com / NH AG's office Author: Adam Greenberg
Article Title: More than 10,000 Utah Food Bank donors notified of breach
Article URL: http://www.scmagazine.com/more-than-10000-utah-food-bank-donors-notified-of-breach/article/435812/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-03	Olympia Hotel Management / Brunswick Hotel & Tavern	ME	8/21/2015	Electronic	Business	Yes - Published #	2,600

Olympia Hotel Management, manager of the Brunswick Hotel & Tavern located at 4 Noble Street, Brunswick, Maine, recently discovered malware on the hotel's computer systems that may have resulted in unauthorized access to name and payment card information. As a recent guest of the hotel, we are writing to provide you with information about this incident, to share the steps that we are taking in response, and to provide you with important information about the steps you can take to reduce the risk of unauthorized use of your personal information.

Attribution 1 Publication: Portland Press Herald / MD AG's office Author:
Article Title: Brunswick Hotel notifies 2,600 guests of possible payment card data breach
Article URL: http://www.pressherald.com/2015/09/02/brunswick-hotel-notifies-guests-of-possible-payment-card-data-breach/

Attribution 2 Publication: VT AG's office Author:
Article Title: Olympia Hotel Management / Brunswick Hotel & Tavern
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Olympia%20Hotel%20Management%20SBN%20to%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-02	Milk Nursingwear	FL	8/20/2015	Electronic	Business	Yes - Unknown #	Unknown

We appreciate your business and value you as a customer. We are writing to inform you that last week Milk Nursingwear discovered that there was an attempt by a person outside of our company to access credit card orders placed on our website between July 13 – August 6, 2015. While there is no evidence that they were successful in accessing and / or extracting information, out of an abundance of caution, we are writing to notify you of this attempt. The information that could have potentially been taken was credit card details, as well as your name, address and email address.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150901-01	Genworth	VA	8/19/2015	Electronic	Business	Yes - Published #	2,500

On July 30, 2015, your insurance agent, Gerald Darringer, notified us that in an attempt to obtain help desk support for his computer, he allowed access to his computer to a third party he thought was a representative of a major on-line retailer. We now believe this third party was not a representative of the retailer, and it is possible that this connection allowed access to the files on his computer. These files may have contained your name, address, date of birth, social security number, banking information as well as policy account numbers and some personal health information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150827-02	Merit Health Northwest Mississippi	MS	8/27/2015	Electronic	Medical/Healthcare	Yes - Published #	846

The release says that on July 1, law enforcement officials notified the hospital that one of their employees was under investigation for identity theft. The hospital opened its own internal investigation, and said it appears this employee, who has since been terminated, “was removing documents from the hospital from February 2013 through June 2015.”

Attribution 1 Publication: pressregister.com Author: Rebekah M. Yearout
Article Title: Merit Health notifies patients of security breach
Article URL: http://www.pressregister.com/article_25c5ba2e-4cf8-11e5-8e64-f32bb07d6ee0.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150827-01	Cancer Care Northwest	WA	8/17/2015	Paper Data	Medical/Healthcare	Yes - Published #	1,426

The PHI of 1,426 Cancer Care Northwest (CCNW) is potentially at risk after the healthcare provider realized that a notebook containing the information was missing. CCNW became aware of the missing item on June 19, 2015, according to a company statement. Information in the notebook included patient names, dates of birth, patient ID numbers, diagnoses, and some treatment information.

Attribution 1 Publication: hhs.gov / healthitsecurity.com Author:
Article Title: Cancer Care Northwest
Article URL: http://healthitsecurity.com/news/possible-health-data-breaches-for-ohio-wash.-providers

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150826-01	Office of Robert Soper, MD	CA	8/26/2015	Electronic	Medical/Healthcare	Yes - Published #	2,000

During a visit to San Francisco On June 27 my car was broken into and my computer stolen, along with camera, suitcases, and other equipment. The computer was an older office desktop I planned to give to my brother. It was hidden in the trunk. The computer contained patient names, dates of birth, some phone numbers, and clinical notes, and e-mails. Addresses, social security numbers, and insurance information were not stored on the stolen computer.

Attribution 1 Publication: CA AG's letter Author:
Article Title: Office of Robert Soper, MD
Article URL: https://oag.ca.gov/system/files/SOPER%20NOTIFICATION%20LETTER_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150825-08	Holiday Inn Harrisburg/Hershey -	MD	8/14/2015	Electronic	Business	Yes - Unknown #	Unknown

Beginning on or about June 28, 2015, current and former guests complained of fraudulent charges on credit cards used to make reservations at the hotel. Upon receipt of these complaints, Milestone immediately launched an investigation to determine the nature and scope of the incident. Milestone reported this incident to its processor and the hotel franchisor.

Attribution 1 Publication: NH AG's office / VT AG's office Author:
Article Title: Holiday Inn Harrisburg/Hershey - Milestone Hospitality Management
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/milestone-hospitality-management-20150814.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150825-07	Rogers Electric	GA	8/21/2015	Electronic	Business	Yes - Unknown #	Unknown

On July 21, 2015, a Rogers employee responsible for various duties in the company's Human Resources department was terminated. Immediately following the employee's termination, Rogers discovered that on July I 0, 2015, the employee had sent copies of payroll documents to their personal email address. These documents contained information relating to current and former employees, including name, Social Security number, and monthly pay amount.

Attribution 1 Publication: NH AG's office Author:
Article Title: Rogers Electric
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/rogers-electrical-20150821.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150825-06	Endocrinology Associates, Inc.	OH	8/14/2015	Electronic	Medical/Healthcare	Yes - Published #	1,400

The provider is currently renovating its location, and is storing patient charts in a rented POD on-site, according to a company statement. Endocrinology Associates realized on the mornings of June 15 and June 19 that the POD padlock had been removed. While an inventory search proved that no patient information was missing, the provider explained that it “cannot confirm with certainty” that no charts were opened, reviewed, or copied.

Attribution 1 Publication: hhs.gov / OCR Author:
Article Title: Endocrinology Associates, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Attribution 2 Publication: hhs.gov / healthitsecurity.com Author:
Article Title: Ohio provider reports missing padlock at rented POD
Article URL: http://healthitsecurity.com/news/possible-health-data-breaches-for-ohio-wash.-providers

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150825-05	**Empi Inc. / DJO LLC**	MN	8/20/2015	Electronic	Medical/Healthcare	Yes - Published #	**160,000**

Empi Inc and DJO, LLC MN Healthcare Provider 160000 08/20/2015 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Empi Inc. / DJO 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
ITRC20150825-04	**Pediatric Group**	IL	8/21/2015	Electronic	Medical/Healthcare	Yes - Published #	**10,000**

Pediatric Group LLC IL Healthcare Provider 10000 08/21/2015 Hacking/IT Incident Network Server

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150825-03	**Totally Promotional**	OH	8/24/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Totally Promotional, an Ohio-based internet seller of imprinted promotional products, is notifying an undisclosed number of customers that attackers forced their way into its systems and gained access to some customer payment card data and other information.

Attribution 1 Publication: scmagazine.com / NH AG's office Author: Adam Greenberg
Article Title: Totally Promotional attack compromises payment cards, other data
Article URL: http://www.scmagazine.com/totally-promotional-attack-compromises-payment-cards-other-data/article/434514/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150825-02	**Department of Human Services / Office of**	CO	8/24/2015	Electronic	Government/Military	Yes - Published #	**3,044**

According to the OIT, 1,622 of the letters were intended for Medicaid recipients and contained personal health information, and 1,069 were intended for Colorado Department of Human Services (CDHS) clients and included Social Security numbers. Another 353 CDHS letters included personally identifiable information such as names, addresses and state identification numbers.

Attribution 1 Publication: esecurityplanet.com Author:
Article Title: Employee Errors Expose PHI, PII, Social Security Numbers
Article URL: http://www.esecurityplanet.com/network-security/employee-error-exposes-phi-pii-social-security-numbers.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150825-01	**Akron Children's Hospital**	OH	8/25/2015	Electronic	Medical/Healthcare	Yes - Published #	**7,664**

Akron Children's Hospital has notified 7,664 patient families that a hard drive of back-up transport voice recordings is lost. The recordings do not contain Social Security numbers or financial information, but some include names and information considered to be protected health information.

Attribution 1 Publication: databreaches.net / hipaajournal.com Author:
Article Title: 7,664 families notified of recordings missing from Akron Children's Hospital
Article URL: http://www.databreaches.net/oh-7664-families-notified-of-recordings-missing-from-akron-childrens-hospital/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150824-06	web.com	FL	8/18/2015	Electronic	Business	Yes - Published #	93,000

About 93,000 Web.com customers may have had their credit card information compromised in a hacking incident discovered five days ago, the company said in a filing with the Securities and Exchange Commission on Tuesday.

Attribution 1 Publication: bizjournals.com Author:
Article Title: Web.com hack reveals credit card details of 93,000 customers
Article URL: http://www.bizjournals.com/jacksonville/news/2015/08/18/web-com-hack-reveals-credit-card-details-of-93-000.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150824-05	University of Rhode Island	RI	8/20/2015	Electronic	Educational	Yes - Unknown #	Unknown

The University of Rhode Island has urged students to change their passwords after a security breach, involving nearly 3,000 current and former student email accounts. URI Spokeswoman Linda Acciardo said the information that was accessed includes email addresses, passwords and dates of birth. The breach did not include any social security numbers or financial information, according to URI.

Attribution 1 Publication: ripr.org Author:
Article Title: URI Reports Data Security Breach
Article URL: http://ripr.org/post/uri-reports-data-security-breach

Attribution 2 Publication: URI website Author:
Article Title: University of Rhode Island
Article URL: http://web.uri.edu/publicsafety/data-security-issue/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150824-04	AutoZone	TN	8/23/2015	Electronic	Business	Yes - Published #	49,967

This afternoon, JM511 announced the hack of the AutoZonePro.com site on Twitter. The linked paste included 49,967 customers' details: billing addresses (street and city), email addresses, hashed passwords, telephone numbers, customers' cities, and dates of birth. Although the passwords were hashed, JM511 provided the password hash in the paste. While no financial data was dumped, JM511 informs DataBreaches.net that he acquired other data concerning AutoZone customer orders that he did not dump. AutoZone may recognize the following fields: ipaddy cc_ccv cc_type currency cc_start cc_issue cc_owner cc_number po_number cc_expires billing_name account_name payment_info billing_city orders_status delivery_name delivery_city last_modified cc_bank_phone

Attribution 1 Publication: databreaches.net Author:
Article Title: 50,000 AutoZone customers' data hacked, exposed (update1)
Article URL: http://www.databreaches.net/50000-autozone-customers-data-hacked-exposed/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150824-03	Volkswagen of Oakland (M&M Automotive Group)	CA	7/27/2015	Electronic	Business	Yes - Unknown #	Unknown

On July 27, 2015, the dealership property was broken into and vandalized. The vandalism involved the theft of a vehicle and boxes of archived files from the secured storage room located on the third floor. We believe that some of the stolen boxes held sold vehicles jackets. Each sold vehicle jacket typically contains copies of the forms signed by the vehicle purchaser including the name, address, phone number, driver's license information, bank account information, car insurance information and information on the vehicle purchased. In some cases where financing is provided in connection with the purchase of a vehicle, the deal jacket will also contain a copy of the consumer's credit application, credit report, pay stubs, job information and references. To the best of our knowledge, the data accessed and embezzled does include private personal information which can be used in identity theft and other criminal activities.

Attribution 1 Publication: CA AG's office Author:
Article Title: Volkswagen of Oakland (M&M Automotive Group)
Article URL: https://oag.ca.gov/system/files/Security%20Breach%20Notice_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150824-02	Buyers Protection Group	GA	7/19/2015	Electronic	Business	Yes - Unknown #	Unknown

On July 19, 2015, a company laptop was stolen from an employee 's car during a large-scale break in of at least 20 vehicles in the Greater Atlanta Area. The incident was immediately reported to the police and a police report was filed. Accordingly, we are working with local law enforcement and Fidelity National Financial's (parent company of BPG) security team to investigate the incident and take appropriate responsive action. In the course of FNF's security team investigation, it was discovered that a file containing your name, address, date of birth and social security number was likely on the laptop at the time of the theft.

Attribution 1 Publication: CA AG's office Author:
Article Title: Buyers Protection Group
Article URL: https://oag.ca.gov/system/files/BPG%20incident_Customer%20Notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150824-01	William W. Backus Hospital	CT	8/23/2015	Electronic	Medical/Healthcare	Yes - Published #	360

The William W. Backus Hospital has sent breach notification letters to 360 individuals alerting them that their Protected Health Information (PHI) may have been viewed by an unauthorized individual. The information potentially viewed includes patient names, medical record numbers, dates of treatment, and information relating to the diagnoses and treatment provided to patients. The hospital confirmed to patients that no Social Security numbers, financial information or insurance details had been disclosed. Individuals affected by the breach had previously visited the hospital's emergency room for treatment.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: POTENTIAL PHI DISCLOSURE AFTER EMPLOYEE WORKS FROM HOME WITH HOSPITAL DATA
Article URL: http://www.hipaajournal.com/potential-phi-disclosure-after-employee-works-from-home-on-hospital-data-8076/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-33	University of Oklahoma, Department of Obstetrics and	OK	7/3/2015	Electronic	Medical/Healthcare	Yes - Published #	7,693

On the June 12, 2015, OU Physicians learned that a laptop had been stolen from a physician's car earlier that day. The laptop had a list of information on it related to two groups of individuals. For one group of individuals, the information included full name, medical record number, date of birth, age, the name and date of a gynecologic or urogynecologic medical procedure, patient account number, and admission and discharge dates for that procedure (if the procedure was an inpatient procedure). Social Security numbers and credit card numbers were not included.

Attribution 1 Publication: databreaches.net / hhs.gov / hipaajourn Author:
Article Title: U. of Oklahoma College of Medicine – Department of Obstetrics & Gynecology notified patients after laptop stolen from physici
Article URL: http://www.databreaches.net/u-of-oklahoma-college-of-medicine-department-of-obstetrics-gynecology-notified-patient

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-32	Special Agents Mutual Benefit Association	MD	7/20/2015	Electronic	Medical/Healthcare	Yes - Published #	1,475

Special Agents Mutual Benefit Association MD Health Plan 1475 07/20/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Special Agents Mutual Benefit Association
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
ITRC20150818-31	T. J. Samson Community Hospital	KY	8/7/2015	Electronic	Medical/Healthcare	Yes - Published #	2,060

T.J. Samson Community Hospital KY Healthcare Provider 2060 08/07/2015 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: T. J. Samson Community 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
ITRC20150818-30	Office of Max M. Bayard, MD, PC	VT	8/7/2015	Electronic	Medical/Healthcare	Yes - Published #	2,000

On August 5, 2015, our offices were broken into and computer devices stolen. As soon as we discovered the theft, we notified law enforcement and are cooperating with their investigation. We also immediately began an investigation to discover what information was on the devices, and determined that your name, Social Security number, and other limited treatment-related information may have been on the devices.

Attribution 1 Publication: hhs.gov / VT AG's office / hipaajournal.c Author:
Article Title: Office of Max M. Bayard, MD, 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
ITRC20150818-29	Baylor College of Medicine	TX	8/7/2015	Paper Data	Medical/Healthcare	Yes - Published #	1,004

A physician's backpack containing five unencrypted portable data drives and a handwritten notebook with the protected health information (PHI) of approximately 1,004 pediatric patients was stolen from an automobile. The types of PHI involved in the breach included names, dates of birth, hospital medical record numbers, types of surgery performed, and treating physicians' names.

Attribution 1 Publication: hhs.gov / OCR Author:
Article Title: Baylor College of Medicine
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-28	Walgreen Co.	IL	8/7/2015	Paper Data	Medical/Healthcare	Yes - Published #	8,345

Walgreen Co. IL Healthcare Provider 8345 08/07/2015 Unauthorized Access/Disclosure Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-27	shorepowerinc.com	CT	7/29/2015	Electronic	Business	Yes - Unknown #	Unknown

On June 19, 2015, we became aware that our web site may have been compromised and promptly took measures to protect the type of information that was involved in the incident. We conducted an investigation and determined the following. On April 23, 2015 without our knowledge or consent, malicious code had been inserted into the functions that process customer payment information through our web site.

Attribution 1 Publication: MD AG's office Author:
Article Title: shorepowerinc.com
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256821.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-26	Boston University	MA	7/10/2015	Electronic	Educational	Yes - Published #	828

In May 2015, a member of the staff of Boston University's Information Systems & Technology Department (IS&T) was contacted by the administrator of a network in Halifax, Nova Scotia who reported that a server on the Boston University networks (the "Server") was attacking the system in Nova Scotia. As a result of this report, the University's Information Security Department initiated an investigation. During the more than month-long complex investigation, investigators learned that a third party had infiltrated the Server and had installed a hacking toolkit, which was responsible for the attacks on the system in Nova Scotia

Attribution 1 Publication: MD AG's office Author:
Article Title: Boston University
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256525.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-25	National American University	SD	6/15/2015	Electronic	Educational	Yes - Unknown #	Unknown

National American University has rigorous policies and protocols in place to maintain the confidentiality of student educational records. Even so, NAU has discovered that some University records were accessed improperly and without authorization. Upon learning of this situation, the University conducted an extensive investigation, and our investigation has revealed that the records at issue may have contained your social security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: National American University
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256480.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-24	LPL Financial	CA	6/30/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On June 11, 2015, we became aware that an LPL Financial advisor employed an unlicensed individual to perform tax and administrative services, but did not notify LPL Financial of this employment arrangement. While employed, the unlicensed individual had access to the clients' accounts. As a result, personal c lient information, including name, date of birth, Social Security number, and LPL Financial account numbers may have been exposed.

Attribution 1 Publication: MD AG's office Author:
Article Title: LPL Financial
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256328.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-23	Fahrenheit Group	VA	7/16/2015	Electronic	Business	Yes - Unknown #	Unknown

On May 26, 2015, during the routine processing of payroll, the Fahrenheit Group discovered discrepancies in the routing and account numbers for certain employees. The
Fahrenheit Group immediately halted the payroll to investigate this issue. The Fahrenheit Group also reached out to its payroll vendor to find out what was happening. Additionally, third party fo rensic investigators were retained to confirm the nature and scope of this incident.

Attribution 1 Publication: MD AG's office Author:
Article Title: Fahrenheit Group
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-255998.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-22	Aon Hewitt / Unum	IL	7/2/2015	Electronic	Business	Yes - Unknown #	Unknown

On or around June 5, 2015, a Reed Elsevier program participant inadvertently accessed an embedded bookmark on a file that was e-mailed to that individual. The file included Social Security numbers for other individuals, who may also be participants in the LTD Program. The file was e-mailed to other Reed Elsevier LTD Program participants. Your Social Security number may have been included.

Attribution 1 Publication: MD AG's office Author:
Article Title: Aon Hewitt / Unum
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/2015/itu-255819.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-21	Nexient LLC	CA	7/10/2015	Electronic	Business	Yes - Unknown #	Unknown

On June 10, 2015, an associate from Nexient's Human Resources department discovered that her personal vehicle was burglarized. Stolen from the automobile was the employee's Nexient issued laptop. The associate promptly reported the theft to local law enforcement and to Nexient. The laptop was password protected at the time of the theft, but it was not encrypted.

Attribution 1 Publication: MD AG's office Author:
Article Title: Nexient LLC
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-255813.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-20	Mid-Atlantic German Shepherd Rescue	DC	7/2/2015	Electronic	Business	Yes - Unknown #	Unknown

On June 8, 2015, an unknown person broke into a car belonging to an employee of Calibre CPA Group, PLLC, an accounting firm retained by the Mid-Atlantic German Shepherd Rescue organization. Among items stolen from the vehicle was a backpack containing a small amount of accounting information, including copies of checks deposited by the German Shepherd Rescue organization. We have reason to believe that one of deposited checks among these copies was written by you to the Mid-Atlantic German Shepherd Rescue.

Attribution 1 Publication: MD AG's office Author:
Article Title: Mid-Atlantic German Shepherd Rescue Association / Calibre CPA Group
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-255594.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-19	Collected Intelligence	NY	6/14/2015	Electronic	Business	Yes - Unknown #	Unknown

On May 14, 2015, a company laptop and case containing your personal information in electronic copy was stolen from company premises. While the laptop was password protected, the electronic files on the laptop were not encrypted. The files may have contained your social security number, date of birth, drivers' license number, and/or home address.
At this tim

Attribution 1 Publication: MD AG's office Author:
Article Title: Collected Intelligence
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256760.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-18	T. Rowe Price Retirement Plan Services	MD	6/16/2015	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you of a situation concerning the compromise of your personal information. As recordkeeper for retirement plans, we have personal information about you related to your eligibility to participate in your [current][former] employer's 40l(k) retirement plan. We were notified by law enforcement a few weeks ago that they found personally identifiable information of several people, including you, in the possession of a former T. Rowe Price employee. This notification to you was delayed at the request of law enforcement.

Attribution 1 Publication: MD AG's office Author:
Article Title: T. Rowe Price Retirement Plan Services
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256530.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-17	State Farm	IL	6/15/2015	Electronic	Business	Yes - Unknown #	Unknown

On the afternoon of Monday, June 8, 2015, an issue was identified that allowed some individuals logged into their online accounts to view another customer's information. We believe this issue was caused by an internal systems update. It was addressed in a matter of hours.

Attribution 1 Publication: MD AG's office Author:
Article Title: State Farm
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256523.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-16	Miami Dade College	FL	6/12/2015	Electronic	Educational	Yes - Unknown #	Unknown

On August 14, 2014, the IRS Task Force alerted MDC to an ongoing investigation involving the theft of personal information belonging to some of MDC's students. MDC has learned that a former employee of MDC, who had authorized access to student records, stole personally identifiable information of current and former MDC students and used the information to help file fraudulent tax returns between February 2013 and June 2014.

Attribution 1 Publication: MD AG's office Author:
Article Title: Miami Dade College
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256519.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-15	Allegis Group	MD	6/2/2015	Electronic	Business	Yes - Unknown #	Unknown

On April 20, 2015, we learned from Equifax that an individual had potentially misused his or her access privileges to reset the account of one Maryland resident of the Company and access personal information associated with the account. The account reset occurred between January 20 15 and February 2015. We have learned the individual is no longer associated with Equifax. The personal information may have included names, home addresses, employee identification numbers, social security numbers, financial information, and employment information including hire date, termination date, total time, and last pay date

Attribution 1 Publication: MD AG's office Author:
Article Title: Allegis Group
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256464.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-14	Asbury Methodist Village Continuing Care Retirement	MD	6/3/2015	Electronic	Business	Yes - Unknown #	Unknown

On May 24, 2015 residents and employees at Asbury Methodist Village Continuing Care Retirement Community ("Community") raised the possibility that their credit and debit card security had been compromised and that one of the Point of Sale (POS) Systems at the Community may have been the common point of use for each of the compromised cards. Asbury management began investigating the use of payment cards and narrowed the likely security breach down to one POS system in the Community.

Attribution 1 Publication: MD AG's office Author:
Article Title: Asbury Methodist Village Continuing Care Retirement Community
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256083.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-13	Office of Deborah Zimmerman, Ph.D., PC	IL	6/9/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On April 13, 2015, a virus infected Dr. Zimmerman's computer and an unauthorized individual may have gained access to her computer for a limited period of time – less than two hours. While patient information was stored in a file, the program used to access the file was not open. The patient information was administrative in nature and appears to have contained patient names, addresses, dates of birth, phone numbers, Social Security numbers, medical insurance and other limited treatment-related information. It did not contain any clinical data which is stored separately and remains secure.

Attribution 1 Publication: MD AG's office Author:
Article Title: Office of Deborah Zimmerman, Ph.D., PC
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256080.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-12	Mid-America Apartment Communities	TN	5/20/2015	Electronic	Business	Yes - Unknown #	Unknown

On April 15, 2015, MAA discovered that a former employee had sold certain names and Social Security numbers of both current and former residents and applicants to an undercover agent for federal law enforcement. MAA has no evidence that this employee ever sold information to individuals who actually misused the information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Mid-America Apartment Communities
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253958.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-11	Pennsylvania State University - Greater	PA	7/24/2015	Electronic	Educational	Yes - Published #	554

During the afternoon of June 9, 2015, Penn State Security Operations and Services, a unit of Information Technology Services at Penn State University, alerted the Penn State Greater Allegheny Campus Information Technology Department that a computer at the campus had been infected with malicious software. This computer contained some historical files which included the following information of 554 individuals: full name and Social Security Number (SSN). Of the 554 individuals appearing in these files, it is Penn State's understanding that 15 of them are Maryland residents.

Attribution 1 Publication: MD AG's office Author:
Article Title: Pennsylvania State University - Greater Allegheny Campus
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256763.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-10	CF Industries	IL	6/2/2015	Electronic	Business	Yes - Unknown #	Unknown

The incident involved the unintentional posting by one of CF Industries' third party vendors of a file that contained certain names, addresses and social security numbers from our accounts payable file to a document sharing web site. The posting took place on December 11, 2014, although CF Industries did not become aware of this accidental posting until May 26, 2015. We took immediate action to ensure the file was deleted that same day from the site.

Attribution 1 Publication: MD AG's office Author:
Article Title: CF Industries
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256096.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-09	North Carolina State University	NC	7/20/2015	Electronic	Educational	Yes - Unknown #	Unknown

On June 16, 2015 North Carolina State University (NC State) learned that data housed on a university computer server was accessed by an unauthorized person. This unauthorized access created the potential for the individual to view certain personal identifying information. You are receiving this letter because a database housed on the implicated server contained a credit card number associated with your name and an expiration date. The credit card was used sometime between 2003 and 2005 for transactions related to NC State's Bioinformatics Research Center. The credit card expiration date listed on the database has expired.

Attribution 1 Publication: MD AG's office Author:
Article Title: North Carolina State University
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-255993.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-08	Department of Human Resources	MD	7/21/2015	Electronic	Government/Military	Yes - Published #	11,549

We are writing to notify you that records of the Maryland Department of Human Resources (DHR) containing your personally identifiable information may have been compromised. The records contained your first and last name, social security number and date of birth, and as a result your personal information may have been exposed to others. We have no reason to believe your information has been used inappropriately and this notice is being sent out of an abundance of caution.

Attribution 1 Publication: MD AG's office Author:
Article Title: Department of Human Resources
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-255992%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-07	Metropolitan Hospitality Group	VA	6/1/2015	Electronic	Business	Yes - Unknown #	Unknown

I write on behalf of my client, Metropolitan Hospitality Group (operator of the Open Road Grill & Icehouse restaurant; the "Restaurant") to inform you of a security incident involving personal information provided to Metropolitan Hospitality Group that may have affected Maryland residents. Metropolitan Hospitality Group is providing public notice to these individuals and outlining some steps they may take to help protect themselves

Attribution 1 Publication: MD AG's office Author:
Article Title: Metropolitan Hospitality Group
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256524.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-06	Defiance Metal Products Co. 401K Plan & Trust / Ascensus	PA	5/27/2015	Electronic	Business	Yes - Unknown #	Unknown

On May 14, 2015, Ascensus, the recordkeeper for the Defiance Metal Products Co 401K Plan & Trust, inadvertently sent a report containing certain sensitive information including names, birth dates, and Social Security numbers to another Ascensus retirement plan client.

Attribution 1 Publication: MD AG's office Author:
Article Title: Defiance Metal Products Co. 401K Plan & Trust
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256466.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-05	Nationstar Mortgage	TX	8/11/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We are writing to inform you of an incident involving your personal information. On July 27th. an email with a copy of your W2 form was inadvertently sent to an employee at Greenlight. The email and its contents has since been deleted from the respective employee's mailbox.

Attribution 1 Publication: CA AG's office Author:
Article Title: Nationstar Mortgage
Article URL: https://oag.ca.gov/system/files/Greenlight%20Incident_CA_%20Notification081015_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-04	Lee's Deli (Sterling M. Enterprises)	CA	8/14/2015	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that unauthorized individuals installed malicious software on computer systems used to process credit card transactions at our Lee's Deli locations at 75 Battery Street in San Francisco, CA and 4200 Bohannon Drive in Menlo Park, CA. While we do not know whether a particular customer's personal information has been or will be misused, we are providing this notice as a precaution to inform potentially affected customers of the incident and to call their attention to some steps they can take to help protect themselves. We sincerely apologize for any frustration or concern this may cause.

Attribution 1 Publication: CA AG's office / databreaches.net Author:
Article Title: Lee's Deli: breach of payment card system at two locations
Article URL: http://www.databreaches.net/lees-deli-breach-of-payment-card-system-at-two-locations/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-03	Department of Corrections	IL	8/15/2015	Electronic	Government/Military	Yes - Published #	1,000

More than 1,000 Social Security numbers belonging to Illinois Department of Corrections employees were inadvertently released in a response to a Freedom of Information Act request.

Attribution 1 Publication: databreaches.net Author:
Article Title: Illinois Dept. of Corrections says personal data of at least 1,000 employees accidentally released in response to FOIA request
Article URL: http://www.databreaches.net/illinois-dept-of-corrections-says-personal-data-of-at-least-1000-employees-accidentally-r

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-02	Department of Health Care Policy and Financing	CO	8/17/2015	Electronic	Government/Military	Yes - Published #	1,622

The Department of Health Care Policy and Financing (the Department) announced today that protected health information was unintentionally disclosed in a recent mailing. Letters were mailed between May 25 and July 5, 2015 and contained protected health information (PHI) of individuals from 1,622 households. The problem was identified on July 1st when a resident notified county workers after receiving a letter not intended for the resident. The technical error was corrected by the Governor's Office of Information Technology on July 5th.

Attribution 1 Publication: databreaches.net / hipaajournal.com / h Author:
Article Title: Colorado notifies Medicaid patients of HIPAA breach
Article URL: http://www.databreaches.net/colorado-notifies-medicaid-patients-of-hipaa-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150818-01	Lawrence General Hospital	MA	8/13/2015	Electronic	Medical/Healthcare	Yes - Published #	2,071

Lawrence General Hospital, Mass. has reported a missing thumb drive containing the Protected Health Information (PHI) of 2,071 individuals. The drive was last used on June 6, 2015, but it has not been seen since. The thumb drive was noticed as being missing on June 9, 2015.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Massachusetts Hospital Reports Missing Unencrypted Thumb Drive
Article URL: http://www.hipaajournal.com/massachusetts-hospital-reports-missing-unencrypted-thumb-drive-8067/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150811-04	Katy Independent School District	TX	8/7/2015	Electronic	Educational	Yes - Published #	11,000

The IRS agent had a flash drive containing almost 12,000 present and former employees' private information, such as birth dates, addresses, and Social Security numbers. But that agent later misplaced that flash drive.

Attribution 1 Publication: databreaches.net / click2houston.com Author:
Article Title: Thousands of Katy ISD employees' info potentially leaked in IRS audit
Article URL: http://www.click2houston.com/news/thousands-of-katy-isd-employees-info-potentially-leaked-in-irs-audit/34604330

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150811-03	Mohu / Green Wave Scientific	NC	8/10/2015	Electronic	Business	Yes - Published #	2,500

Between June 3, 2015 and July 28, 2015 ("Affected Dates"), Mohu's computer systems were compromised by a hacker who penetrated Mohu's security systems, inserted malicious code into the systems, and removed sensitive data, including the names, addresses, email addresses, phone numbers and credit card information (number, expiration date and CVV code) of approximately 2,500 customers who purchased products from the www.gomohu.com website during the Affected Dates.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150811-02	SterlingBackcheck	NY	8/7/2015	Electronic	Business	Yes - Published #	100,000

On May 29, 2015, a password-protected laptop was stolen from a SterlingBackcheck employee's vehicle. The employee reported the theft to our office, and we launched an investigation to determine what information may have been stored on the laptop at the time of the theft. While our investigation is ongoing, we've determined a file containing your name, Social Security number, and date of birth may have been stored on the laptop at the time of the theft. We are unaware of any actual or attempted misuse of this information, and there is no indication the data that may have been stored on the laptop was the target of the theft.

Attribution 1 Publication: databreaches.net Author:
Article Title: Update: SterlingBackcheck breach impacted 100,000
Article URL: http://www.databreaches.net/update-sterlingbackcheck-breach-impacted-100000/

Attribution 2 Publication: NH AG's office / MD AG's office Author:
Article Title: CoWorx Human Resources
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/coworx-staffing-20150817.pdf

Attribution 3 Publication: NH AG's office Author:
Article Title: SterlingBackcheck / Davis Companies
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/davis-companies-20150803.pdf

Attribution 4 Publication: CA AG's office / NH AG's office Author:
Article Title: SterlingBackcheck
Article URL: https://oag.ca.gov/system/files/Exhibit%20A_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150811-01	Positive Adjustments	UT	8/10/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Another case of illegal dumping of medical records has been reported, this time involving a Utah drug and rehabilitation clinic, Positive Adjustments. The company went out of business approximately 6 months ago; however medical records were discovered in a dumpster outside the abandoned clinic – at 4548 South Atherton, Taylorsville, by a contractor employed by Dr. Scott Cold, DDS on Friday last week.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: ILLEGAL DUMPING OF MEDICAL RECORDS EXPOSES PHI OF OHIO DRUG REHAB CLINIC PATIENTS
Article URL: http://www.hipaajournal.com/positive-adjustments-illegal-dumping-of-medical-records-8063/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150806-02	Richmond Public Schools	VA	8/6/2015	Paper Data	Educational	Yes - Unknown #	Unknown

If you teach or have taught for Richmond Public Schools, your colleagues may have access to your personal information. The disclosure that the RPS Human Resources Department is failing to guard confidential records came from a former teacher who found her personnel file contained information it should not have, including Social Security numbers of other teachers.

Attribution 1 Publication: databreaches.net / Richmondfreepress.c Author:
Article Title: Confidentiality breach: Teacher's file contains personal info on others
Article URL: http://richmondfreepress.com/news/2015/aug/05/confidentiality-breach-teachers-file-contains-pers/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150806-01	Mama Mio US	CA	7/28/2015	Electronic	Business	Yes - Unknown #	Unknown

We are sorry to inform you that we have been the victim of a cyber-attack on our website. Given the nature of the attack, we have to assume it has resulted in the loss of your personal data. As soon as we became aware of the attack on 28th July, we commissioned a forensic team to locate the malware, identify the compromised data and prevent any further loss. In accordance with our regulatory obligations and our duty of care for our customers, we are contacting all customers who ordered from mioskincare.com from 29th April to 28th July 2015 to ensure we protect every Mio customer.

Attribution 1 Publication: CA AG's office Author:
Article Title: Mama Mio US
Article URL: https://oag.ca.gov/system/files/MM%20US%20letter%20to%20customers%20-%20data%20breach_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-14	Woodbury Financial Services	CA	7/27/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On May 28, 2015, a Woodbury Registered Representative's laptop computer was accessed by an unauthorized indi vidual as part of a phishing scam. The laptop computer contained spreadsheets that included information belonging to New Hampshire residents. It cannot be confirmed if the information was accessed or viewed by the unauthorized individual. The laptop computer was scanned, cleaned and deemed free of viruses. The information contained the New Hampshire residents ' names, Social Security numbers and/or driver's license numbers.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Woodbury Financial Services
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/woodbury-financial-20150727.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-12	University of Connecticut School of Engineering	CT	7/31/2015	Electronic	Educational	Yes - Unknown #	Unknown

The School of Engineering immediately notified faculty, staff, students, visitors, and emeriti – as well as roughly 1,800 users of the Lync instant communication tool used across the University at the time – that their log-in credentials had potentially been compromised, and recommended that those individuals change their passwords.

Attribution 1 Publication: databreaches.net Author:
Article Title: UConn Discloses Data Breach at School of Engineering
Article URL: http://www.databreaches.net/uconn-discloses-data-breach-at-school-of-engineering-that-began-in-2013/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-11	VA Black Hills Health Care System	SD	8/1/2015	Paper Data	Government/Military	Yes - Published #	1,100

Human error strikes the VA system again. Seth Tupper reports that someone at the VA Black Hills Health Care System mistakenly dumped a box containing 1,100 veterans' files into a dumpster on May 15. The error occurred during an office move (a problem we've seen before in other cases).

Attribution 1 Publication: databreaches.net Author:
Article Title: Files of 1,100 veterans thrown in dumpster at Hot Springs VA
Article URL: http://www.databreaches.net/files-of-1100-veterans-thrown-in-dumpster-at-hot-springs-va/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-10	Tremco	OH	7/29/2015	Electronic	Business	Yes - Unknown #	Unknown

On June 17, 2015, a human resources employee discovered, during a business trip, that he had left his Company-issued laptop computer in the pocket of his airplane seat. The employee promptly notified the major airline on which he had flown and remained in contact with the airline in an effort to recover the laptop. The laptop has not yet been recovered.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-09	Department of Child Safety	AZ	8/4/2015	Paper Data	Government/Military	Yes - Unknown #	Unknown

A batch of documents from the Department of Child Safety was found in Kingman. They contained personal information including names and social security numbers. the documents reportedly contained detailed descriptions of investigations.

Attribution 1 Publication: databreaches.net / fox10phoenix.com Author:
Article Title: Kingman resident finds DCS investigation documents in dumpster
Article URL: http://www.databreaches.net/az-kingman-resident-finds-dcs-investigation-documents-in-dumpster/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-08	Prima CARE, PC	MA	7/29/2015	Paper Data	Medical/Healthcare	Yes - Published #	1,651

However this week, a (now former) employee of a healthcare provider has exposed patient records in a rather atypical way. The individual in question was an employee of Prima CARE, P.C, a healthcare provider based in New England. That individual breached HIPAA and hospital rules by maintaining patient records without the knowledge of his or her employer, and apparently dumped the files when they were no longer required.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: PRIMA CARE DISCOVERS IMPROPER DUMPING OF PHI: 1,651 PATIENTS AFFECTED
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
ITRC20150804-07	Urology Associates, Professional Corporation	MT	7/24/2015	Paper Data	Medical/Healthcare	Yes - Published #	6,500

Offsite storage of paper medical records may be convenient if facility space is limited; but the decision to store records offsite may prove to be a costly, as Kailspell-based healthcare provider, Urology Associates recently discovered. The company had taken advantage of a local storage facility and rented a unit to store boxes of old medical records. Unfortunately, the facility was recently burgled.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Urology Associates, Professional Corporation
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
ITRC20150804-06	Advanced Radiology Consultants	CT	8/2/2015	Electronic	Medical/Healthcare	Yes - Published #	855

On July 24, Advanced Radiology Consultants, LLC., announced a data security event that exposed the data of a small subset of its patients. The breach report submitted to the Department of Health and Human Services' Office for Civil Rights indicates 855 patients have been affected. The data breach was caused when an employee of the company emailed a list of patients' PHI to a personal email account. The list of data included patient names, telephone numbers, dates of birth, balance information, patient identification numbers, examination results, treatment information, appointment dates and times, appointment notes, referring physician names, insurance provider, and insurance identification numbers.

Attribution 1 Publication: hipaajournal.com / databreaches.net Author:
Article Title: Unauthorized Email Exposes PHI of 855 Advanced Radiology Consultants Patients
Article URL: http://www.hipaajournal.com/unauthorized-email-exposes-phi-of-855-advanced-radiology-consultants-patients-8051/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-05	Siouxland Anesthesiology Pain Clinic	SD	8/4/2015	Electronic	Medical/Healthcare	Yes - Published #	13,000

A foreign hacker is responsible for causing the recently discovered Siouxland Pain Clinic data breach, according to a statement released by the healthcare provider's attorney. The hacker managed to infiltrate the healthcare provider's computer network, and potentially obtained the Protected Health Information of an undisclosed number of its patients.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Foreign Hacker Responsible for Siouxland Pain Clinic Data Breach
Article URL: http://www.hipaajournal.com/foreign-hacker-responsible-siouxland-pain-clinic-data-breach-8056/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-04	Sioux Falls VA Health Care System	SD	8/4/2015	Paper Data	Government/Military	Yes - Published #	1,111

The Department of Veterans Affairs has announced the potential exposure of 1,111 veteran health records after files containing Personally Identifiable Information (PII) and Protected Health Information (PHI) were accidentally tossed in a dumpster. The files were thrown out with regular waste by an employee of the VA Hot Springs Hospital in South Dakota on Friday, May 15, during a move to a different location. The files were mistaken for regular rubbish, and would have remained in the publically-accessible dumpster were it not for a vigilant employee who noticed the dumped files two days later.

Attribution 1 Publication: hipaajuornal.com Author:
Article Title: HIPAA Breach: 1,111 Veteran Records Improperly Dumped
Article URL: http://www.hipaajournal.com/hipaa-breach-1111-veteran-records-improperly-dumped-8058/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-03	Office of Orlantino Dyoco, MD	CA	7/13/2015	Electronic	Medical/Healthcare	Yes - Published #	9,000

On June 2, 2015, Dr. Dyoco opened his office and found the office had been burglarized. Several computers had been stolen, containing patient information used for billing, which included: Names and addresses, Birth dates, telephone numbers, Insurance numbers, treatment codes, and billing information

Attribution 1 Publication: CA AG's office Author:
Article Title: Office of Orlantino Dyoco, MD
Article URL: https://oag.ca.gov/system/files/dyoco%20notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-02	North East Medical Services	CA	7/30/2015	Electronic	Medical/Healthcare	Yes - Published #	69,246

We have learned that personal information about you and some of our other patients may have been disclosed, including one or more of the following: your name, date of birth, gender, contact information, payer/insurer and limited personal health information. It is important to note that no Social Security number, credit card information or actual medical record was involved. However, on July 11, 2015, an employee's vehicle was broken into, and the employee's work laptop belonging to NEMS was stolen from the trunk of a locked vehicle, along with other items.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: North East Medical Services HIPAA Breach Reported: 69,246 Affected
Article URL: http://www.hipaajournal.com/north-east-medical-services-hipaa-breach-69246-8055/

Attribution 2 Publication: CA AG's office / hipaajournal.com Author:
Article Title: North East Medical Services
Article URL: https://oag.ca.gov/system/files/NEMS%20Letter_LimitedData_SHORT_final_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150804-01	**Orange County Employees Association**	CA	7/31/2015	Electronic	Business	Yes - Unknown #	**Unknown**

On July 23, 2015, we determined that one or more attackers had successfully penetrated parts of the OCEA network and potentially gained access to personal information, including yours, that may have included: name, address, date of birth, Social Security number, driver's license number, payroll information, dental, vision, life and disability enrollment information, retirement status, information concerning dependents and usernames and passwords. The ongoing investigation suggests that the attack has been underway since at least June 5, 2015.

Attribution 1 Publication: CA AG's office Author:
Article Title: Orange County Employees Association
Article URL: https://oag.ca.gov/system/files/AG%20Sample%20Notice%20073115_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150730-02	**Hanesbrands, Inc.**	NC	7/30/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Hanesbrands Inc. said Wednesday that a customer order database was breached by a hacker in June, compromising information for about 900,000 online and telephone customers. The hacker gained access to general customer information through the company's website by posing as a "guest" customer checking an order, meaning they weren't registered on the site. The hacker was able to get information including addresses, phone numbers and last four digits of a credit or debit card of other customers, Hanesbrands spokesman Matt Hall said.

Attribution 1 Publication: journalnow.com / databreaches.net Author:
Article Title: Hanesbrands database hacked
Article URL: http://www.journalnow.com/business/business_news/local/hanesbrands-database-hacked/article_543b338e-3664-11e5

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150730-01	**East Bay Perinatal Medical Associates**	CA	7/29/2015	Electronic	Medical/Healthcare	Yes - Published #	**1,494**

An East Bay Perinatal Medical Associates data breach has recently been announced, in which names and dates of birth of patients have been exposed. The healthcare provider is now sending notification letters to patients warning them of the privacy violation. The healthcare provider became aware of the breach of personal information on June 2, 2015. The data breach was not uncovered by the hospital; instead it was brought to the attention of East Bay Perinatal Medical Associates (EBPMA) by the Berkeley Police Department as a result of a totally unrelated investigation. 1,494 individuals have been affected according to the HHS breach report.

Attribution 1 Publication: CA AG's letter / hipaajournal.com Author:
Article Title: East Bay Perinatal Medical Associates
Article URL: http://www.hipaajournal.com/east-bay-perinatal-medical-associates-data-breach-8050/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150729-01	**McLean Hospital**	MA	7/29/2015	Electronic	Medical/Healthcare	Yes - Published #	**12,673**

Massachusetts-based McLean Hospital announced this week that it had suffered from a health data breach, potentially affecting 12,600 individuals. McLean discovered on May 29, 2015 that four unencrypted backup data tapes were missing, according to a company statement. The information was not from the hospital's medical record system, but involved data that was being kept as part of a research program at the Harvard Brain Tissue Resource Center (HBTRC).

Attribution 1 Publication: healthitsecurity.com Author: Elizabeth Snell
Article Title: McLean Hospital Reports Health Data Breach, Affects 12,600
Article URL: http://healthitsecurity.com/news/mclean-hospital-reports-health-data-breach-affects-12600

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-13	**North Dakota Worker's Compensation**	ND	6/12/2015	Electronic	Business	Yes - Unknown #	**Unknown**

A state server containing information from North Dakota's workers' compensation agency was breached, but it's unlikely any personal information was stolen, state officials announced Friday. Mike Ressler, the chief information officer at the state Information Technology Department, said unusual activity was found on a server on May 29 that contains data from the state Workforce Safety and Insurance agency. The server was secured and data was locked down.

Attribution 1 Publication: databreaches.net Author:
Article Title: Seek and ye shall find: North Dakota breach affecting state employees and volunteers bigger than originally realized
Article URL: http://www.databreaches.net/seek-and-ye-shall-find-north-dakota-breach-affecting-state-employees-and-volunteers-bi

Attribution 2 Publication: washingtontimes.com Author:
Article Title: Officials say data breach identified on state server
Article URL: http://www.washingtontimes.com/news/2015/jun/12/officials-say-data-breach-identified-on-state-serv/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-12	Indiana Department of Revenue	IN	7/18/2015	Electronic	Government/Military	Yes - Published #	1,262

Indiana Department of Revenue, 1,262, cause unavailable.

Attribution 1 Publication: indystar.com / IN AG's office Author:
Article Title: Indiana's top 10 data breaches so far this year
Article URL: http://www.indystar.com/story/money/2015/07/18/indianas-top-10-data-breaches-so-far-year/30360027/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-11	City of Amherst	MA	7/22/2015	Electronic	Educational	Yes - Unknown #	Unknown

The personal information of some Amherst, Massachusetts, residents has been compromised through the town's website. Those Amherst residents who may have been affected by the data breach received letters recently alerting them to the issue. Town Finance Director Sandy Pooler says the town discovered it in late June.

Attribution 1 Publication: nepr.net Author:
Article Title: Data Breach Affects Some Amherst Residents
Article URL: http://nepr.net/news/2015/07/22/data-breach-affects-some-amherst-residents/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-10	Mayo Clinic Health System - Red Wing	MN	7/13/2015	Electronic	Medical/Healthcare	Yes - Published #	601

Mayo Clinic Health System- Red Wing MN Healthcare Provider 601 07/13/2015 Unauthorized Access/Disclosure Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: Mayo Clinic Health System - Red Wing
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
ITRC20150728-09	Massachusetts General Hospital	MA	7/8/2015	Electronic	Medical/Healthcare	Yes - Published #	648

The latest Massachusetts General Hospital data breach exposed the data of 648 patients, and included patient names, laboratory test results and a limited number of Social Security numbers, although no insurance information or financial data were exposed. The security incident involved an email that was inadvertently sent to an incorrect recipient; potentially disclosing patient data. The error was identified promptly and the hospital made several attempts to recall the message, but those attempts proved to be unsuccessful.

Attribution 1 Publication: hipaajournal.com / NH AG's office Author:
Article Title: Massachusetts General Hospital
Article URL: http://www.hipaajournal.com/email-error-massachusetts-general-hospital-data-breach-8052/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-08	Maricopa Special Health Care District - Integrated Health	AZ	7/14/2015	Electronic	Medical/Healthcare	Yes - Published #	633

A medical resident lost an unencrypted thumb drive that contained the names, dates of birth, and clinical information or diagnoses of 633 patients selected for a chart review. The covered entity (CE), Maricopa Integrated Health System, provided breach notification to HHS, affected individuals, and the media.

Attribution 1 Publication: hhs.gov / OCR Author:
Article Title: Maricopa Special Health Care District - Integrated Health System
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-07	**Amsterdam Nursing Home Corporation**	NY	7/10/2015	Paper Data	Medical/Healthcare	Yes - Published #	**621**

On January 31, 2015, a fire at the CitiStorage storage facility in Brooklyn, NY, destroyed a secure warehouse where Amsterdam stored some of its documents. After the fire, there was an investigation as to whether the documents were destroyed and, on April 20, 2015, as a result of that investigation, the warehouse owner certified that all of Amsterdam's documents in that warehouse were destroyed in the fire. However, in a letter to Amsterdam on June 2, 2015, the warehouse owner informed Amsterdam for the first time that, after the fire, some documents were found outside of the warehouse.

Attribution 1 Publication: hhs.gov / MD AG's office Author:
Article Title: Amsterdam Nursing Home Corporation
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu255807.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-06	**Healthfirst**	NY	7/24/2015	Electronic	Medical/Healthcare	Yes - Published #	**5,338**

On May 27, 2015, Healthfirst was informed by the Department of Justice ("DOJ") that an individual who perpetrated a fraud against Healthfirst may have stolen information about Healthfirst's patients from Healthfirst's online portal. Healthfirst had discovered that it was the victim of fraud in 2013, notified the DOJ and cooperated with the DOJ's investigation, which resulted in the perpetrator being charged with fraud. During its investigation, the DOJ discovered that the perpetrator had gained access to some member information and recently notified Healthfirst of that fact. On July 10, 2015, we determined that the perpetrator gained access to certain Healthfirst members' personal information between April 11, 2012 and March 26, 2014.

Attribution 1 Publication: databreaches.net / Healthfirst / hhs.gov Author:
Article Title: Healthfirst notifying 5,300 members whose data were stolen between 2012-2014
Article URL: http://www.databreaches.net/healthfirst-notifying-5300-members-whose-data-were-stolen-between-2012-2014/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-05	**Vision Nissan**	NY	7/24/2015	Paper Data	Business	Yes - Unknown #	**Unknown**

The Binghamton Attorney General's Office is advising people to be careful when giving sensitive information to businesses. On Tuesday, Dona Olsen – director of Little Mews Rescue in Norwich – discovered large amounts of personal information in the dumpster behind her business while taking out trash. The information was originally given to Vision Nissan of Webster, NY. The documentation had been placed in the dumpster, not shredded, after the mobile car dealership from Vision had done business in Norwich.

Attribution 1 Publication: databreaches.net / WBNG.COM Author:
Article Title: Personal documents found in Norwich dumpster
Article URL: http://www.wbng.com/news/video/Personal-documents-found-in-Norwich-dumpster-318491251.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-04	**Scient Federal Credit Union**	CT	7/28/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

Add Scient Federal Credit Union to the list of those exposing employee information due to an email error. The error occurred on July 14, and resulted in an unspecified number of employees' details being sent to a prospective employee. The information, which was sent by secure email, included name, Social Security number, address, amount or percentage of 401k contribution, and year-to-date hours and pay.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: Credit union email gaffe exposes employee information
Article URL: http://www.databreaches.net/credit-union-email-gaffe-exposes-employee-information/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-03	OhioHealth Riverside Methodist Hospital	OH	7/28/2015	Electronic	Medical/Healthcare	Yes - Published #	1,006

The data stored on the portable storage device related to valve-replacement candidates and research subjects who had taken part in value replacement projects between July, 2010 and December, 2014. The data stored on the portable storage device included patient names, addresses, dates of birth, physician names, medical record numbers, insurance information, types of medical procedures performed and treatment dates. 30 Social Security numbers have also potentially been exposed.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: OHIOHEALTH REPORTS LOSS OF FLASH DRIVE CONTAINING 1,006 PROTECTED HEALTH RECORDS
Article URL: http://www.hipaajournal.com/ohiohealth-reports-loss-of-flash-drive-containing-1006-protected-health-records-8045/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-02	HSBC Mortgage Service Center	VA	6/22/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently became aware of an incident where your account details were sent in error to a commercial entity not associated with HSBC. The documentation included your name, account number, property address, loan and payment details. We have been informed that the third party recipient did not view your data and your data has been deleted. HSBC takes this very seriously and the security of your information is very important to us.

Attribution 1 Publication: CA AG's office / MD AG's office Author:
Article Title: HSBC Mortgage Service Center
Article URL: https://oag.ca.gov/system/files/Cust%20Notif%20Template%20for%20Regs%20IDGrd_1%20Revised%207-23-2015_0.pd

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150728-01	Ransomed Heart Ministries	CO	7/17/2015	Electronic	Business	Yes - Unknown #	Unknown

This illegal hack did not affect credit cards or debit cards used to make donations, pay event registration fees or pay for RH Tribe membership. On June 15, 2015, we first became aware of a possible breach when it was reported to us from our website hosting company that our website had been manipulated by hackers. By the time we were made aware of the possible breach, our website hosting company had addressed it. After we learned of the report, we took immediate action to confirm our website is secure and we engaged a forensic IT firm to assist us in determining how this occurred.

Attribution 1 Publication: VT AG's office Author:
Article Title: Ransomed Heart
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Ransomed%20Heart%20Ministries%20SBN%20to%20C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150727-01	Golden 1 Credit Union	CA	7/30/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We have discovered that a person employed by us from early April to mid-June of this year appears to have engaged in unauthorized activity involving a small number of member accounts. The personal information available for viewing by this person included full name, social security number, driver's license number and other financial information. Our records indicate that this person viewed your account, most likely as part of their job duties.

Attribution 1 Publication: CA AG's office Author:
Article Title: Golden 1 Credit Union
Article URL: https://oag.ca.gov/system/files/Notification%20template%207.24.15_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150721-07	Alfa Specialty Insurance Corporation / Alfa Vision	TN	7/21/2015	Electronic	Business	Yes - Published #	86,000

Alfa Specialty Insurance Corporation and Alfa Vision Insurance Corporation are notifying around 86,000 individuals that their personal information was inadvertently made accessible to the internet. How many victims? Around 86,000.
What type of personal information? Names, addresses, dates of birth, driver's license numbers and Social Security numbers.

Attribution 1 Publication: scmagazine.com Author: Adam Greenberg
Article Title: Alfa Insurance: data on 86K individuals inadvertently made accessible to internet
Article URL: http://www.scmagazine.com/alfa-insurance-data-on-86k-individuals-inadvertently-made-accessible-to-internet/article/4

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150721-06	Citizens Bank	RI	7/17/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We are writing to inform you that due to a security incident at the Cambridge, MA ATM. your ATM/Debit card may have been compromised. Appropriate measures were taken to secure the ATM upon discovery of the incident The information that may have been compromised includes your name, ATM/Debit card number, PIN and card expiration date.

Attribution 1 Publication: VT AG's office Author:
Article Title: Citizens Bank
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Citizens%20Financial%20Group%20SBN%20to%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150721-05	Atkinson, Andelson, Loya, Ruud & Romo	CA	4/23/2015	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you of an incident involving the theft of a laptop computer owned by an attorney from our law firm that may have contained some of your personal information. We want you to know what happened in this incident, the steps we are taking to protect you, to provide you with additional information that we hope you will find helpful, and contact information should you have any questions. On April 23, 2015, a personal laptop belonging to a member of our law firm was stolen while the attorney was a passenger on the MTS Trolley in downtown San Diego. We have been working with law enforcement but, to date, they have been unable to locate the stolen laptop computer.

Attribution 1 Publication: CA AG's office Author:
Article Title: Atkinson, Andelson, Loya, Ruud & Romo
Article URL: https://oag.ca.gov/system/files/Atkinson%2C%20Andelson%2C%20Loya%2C%20Ruud%20%26%20Romo%20Notice_0.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150721-04	Office of Richard Berger, CPA	CA	6/25/2015	Electronic	Business	Yes - Unknown #	Unknown

I am very sorry to inform you that three external hard drives were stolen from my home in the weeks prior to June 25, 2015, when I discovered the theft. These drives may have contained your personal information including your name, tax information, Social Security number and in some instances bank and investment account information. If you provided information about dependents, beneficiaries, employees or contractors, their names and Social Security number(s) may have been exposed as well. I have notified the Oakland Police Department, but to date the stolen hard drives have not been recovered.

Attribution 1 Publication: CA AG's office Author:
Article Title: Office of Richard Berger, CPA
Article URL: https://oag.ca.gov/system/files/RichardBergerCPAAdr3prf_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150721-03	Department of Human Services Division of Aging	GA	7/8/2015	Electronic	Government/Military	Yes - Published #	2,983

Approximately 3,000 members of the Community Care Services Program of Georgia's Department of Human Services Division of Aging Services (GDHSDAS) have been sent breach notification letters to advise them that a limited amount of their Protected Health Information (PHI) has been accidentally exposed.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Department of Human Services
Article URL: http://www.hipaajournal.com/georgia-division-of-aging-services-data-breach-affects-3000-8040/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150721-02	Integral Health Plan, Inc.	FL	7/10/2015	Paper Data	Medical/Healthcare	Yes - Published #	7,549

Integral Health Plan, Inc. FL Health Plan 7549 07/10/2015 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Mailing Error Exposes PHI of Integral Health Plan Members
Article URL: http://www.hipaajournal.com/mailing-error-exposes-phi-of-integral-health-plan-members-8034/

Attribution 2 Publication: hhs.gov Author:
Article Title: Integral Health Plan, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150721-01	St. John's Episcopal Hospital (Episcopal Health Services)	NY	6/25/2015	Electronic	Medical/Healthcare	Yes - Published #	509

Episcopal Health Services Inc. d/b/a St. John's Episcopal Hospital NY Healthcare Provider 509 06/25/2015 Theft Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: St. John's Episcopal Hospital (Episcopal Health Services)
Article URL: Episcopal Health Services Inc. d/b/a St. John's Episcopal Hospital NY Healthcare Provider 509 06/25/2015 Theft Electr

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150720-02	Rite-Aid / PNI Digital Media	RI	7/20/2015	Electronic	Business	Yes - Unknown #	Unknown

CVS, Rite-Aid, Sam's Club, Walmart Canada and other large retail chains have suspended their online photo services following a suspected hack attack against a third-party service provider that may, in some cases, have resulted in the compromise of payment card data.

Attribution 1 Publication: bankinfosecurity.com / CA AG's office Author:
Article Title: More Retailers Hit by New Third-Party Breach?
Article URL: http://www.bankinfosecurity.com/more-retailers-hit-by-new-third-party-breach-a-8416?rf=2015-07-20-eb&mkt_tok=3Rk

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150720-01	CVS - Photo site	RI	7/20/2015	Electronic	Business	Yes - Unknown #	Unknown

CVS has temporarily shut down its CVS Photo website after one of its vendors may have been breached. CNNMoney pointed out that the vendor, PNI Digital Media, was hacked last year and lost 1.2 million credit cards.

Attribution 1 Publication: mspmentor.net Author:
Article Title: IT Security Stories to Watch: CVS Investigates Data Breach
Article URL: http://mspmentor.net/managed-security-services/072015/it-security-stories-watch-cvs-investigates-data-breach

Attribution 2 Publication: bostonglobe.com / CA AG's office Author:
Article Title: CVS confirms data breach at photo site this summer
Article URL: https://www.bostonglobe.com/business/2015/09/11/cvs-confirms-data-breach-photo-site-this-summer/xc7mG3YFVgkK

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150717-01	UCLA Health	CA	7/17/2015	Electronic	Medical/Healthcare	Yes - Published #	4,500,000

University of California (UCLA) Health has been hit by a cyberattack that exposed the data of about 4.5 million people in the region. The organization said Friday that a network containing personal and medical information was accessed by unknown hackers, including names, addresses, Social Security numbers and medical data -- such as condition, medications, procedures, and test results.

Attribution 1 Publication: zdnet.com / CA AG's office / NH AG's of Author:
Article Title: UCLA Health hit by hack; medical data on 4.5 million people exposed
Article URL: http://www.zdnet.com/article/ucla-health-hit-by-hack-millions-affected/?tag=nl.e589&s_cid=e589&ttag=e589&ftag=TRE

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150715-02	Ohio University Hospitals	OH	7/10/2015	Electronic	Medical/Healthcare	Yes - Published #	300

An Ohio University Hospitals Elyria Medical Center worker has been fired for inappropriately accessing the medical records of patients while employed at the hospital. Alicia Reale, a spokesperson for the hospital, announced yesterday that the medical records of approximately 300 patients had potentially been improperly accessed by an employee of the hospital. The data breach resulted in Protected Health Information (PHI) potentially being viewed and copied.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Ohio University Hospitals Worker Fired for Improper EHR Access
Article URL: http://www.hipaajournal.com/ohio-university-hospitals-worker-fired-improper-ehr-access-8018/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150715-01	Howard (University) Hospital	DC	7/11/2015	Electronic	Medical/Healthcare	Yes - Published #	1,445

Howard Hospital in Washington D.C has announced a mailing error resulted in letters containing patient names, account numbers and the dates of past visits being sent to the wrong recipients.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Mailing Error Causes Howard University Privacy Breach
Article URL: http://www.hipaajournal.com/mailing-error-causes-howard-university-privacy-breach-7021/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150714-05	Jenkinson's Breakwater Beach Waterpark	NJ	7/9/2015	Electronic	Business	Yes - Unknown #	Unknown

Hundreds of documents containing personal information of some employees at Jenkinson's Breakwater Beach Waterpark at Casino Pier in Seaside Heights have been available online to anyone who clicks in the right place, Bamboozled has learned. The documents include copies of Social Security cards, driver's licenses, birth certificates, passports, student IDs, tax forms, seasonal work agreements, minor consent forms and employment eligibility forms from the Department of Homeland Security.

Attribution 1 Publication: nj.com Author:
Article Title: Jenkinson's Breakwater Beach Waterpark
Article URL: http://www.nj.com/business/index.ssf/2015/07/bamboozled_breakwater_beach_security_breach_puts_h.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150714-04	Latex Construction Company	GA	7/7/2015	Electronic	Business	Yes - Unknown #	Unknown

On June 2, 2015, a Safety Coordinator for Latex Construction discovered that his vehicle had been burglarized, while his truck was parked at one of our work sites. The burglar stole the employee's Latex Construction issued laptop and his personal iPad. The information on the laptop and iPad was not password protected or encrypted. Upon learning of the theft, we immediately launched an internal investigation. We contacted local law enforcement, but the laptop and iPad have not been recovered to date.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: Latex Construction Company
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Latex%20Construction%20SBN%20to%20Consumer.p

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150714-03	Arkansas Blue Cross and Blue Shield / Treat Insurance	AR	7/14/2015	Electronic	Medical/Healthcare	Yes - Published #	560

Arkansas Blue Cross and Blue Shield is taking steps to protect its members and applicants from identity theft after an independent insurance agency was broken into last month. Treat Insurance Agency reported a break-in at its North Little Rock office on June 16, 2015. Two computers, which stored information from 560 Arkansas Blue Cross applicants and members dating back to October 1, 2012, were reported stolen.

Attribution 1 Publication: databreaches.net Author:
Article Title: Arkansas Blue Cross and Blue Shield offering credit protection to members affected by computer theft
Article URL: http://www.databreaches.net/arkansas-blue-cross-and-blue-shield-offering-credit-protection-to-members-affected-by-c

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150714-02	Insurance Services Office	NJ	7/13/2015	Electronic	Business	Yes - Unknown #	Unknown

We have been advised by the Prosecutor's office that your personal information may have been viewed by unauthorized individuals. The information that may have been viewed includes: your contact information, date of birth, Social Security number, insurance policy number, and driver's license number.

Attribution 1 Publication: CA AG's office / MD AG's office Author:
Article Title: Insurance Services Office
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-256526.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150714-01	Department of Corrections and Rehabilitation	CA	5/7/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

On May 7, 2015, we discovered that the Gate Clearance document you submitted to Mule Creek State Prison was electronically scanned and stored to a computer folder where employees outside of Plant Operations may have been able to read it. The document contained your name, Driver License number and Social Security number. Immediately upon discovery, access to the folder was secured to only allow access to the Plant Operations employees.

Attribution 1 Publication: CA AG's office Author:
Article Title: Department of Corrections and Rehabilitation
Article URL: https://oag.ca.gov/system/files/CDCR%20MCSP%20-%20Privacy%20Breach_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150713-07	Army National Guard	VA	7/11/2015	Electronic	Government/Military	Yes - Published #	850,000

The U.S. Army National Guard experienced their own personnel data breach, they announced Friday. The data breach includes current and former soldiers' names, full Social Security numbers, dates of birth and home addresses.

Attribution 1 Publication: washingtonexaminer.com Author:
Article Title: New data breach: Army National Guard
Article URL: http://www.washingtonexaminer.com/army-national-guard-suffers-its-own-data-breach/article/2568084

Attribution 2 Publication: infosecurity-magazine.com Author: Tara Seals
Article Title: Army National Guard Exposes 850K Service Member Records
Article URL: http://www.infosecurity-magazine.com/news/national-guard-exposes-850k-member/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150713-06	Rite Aid	PA	6/5/2015	Electronic	Business	Yes - Unknown #	Unknown

On April 30, we learned from Equifax that an individual had potentially misused his or her access privileges to reset the accounts of two New Hampshire residents and access personal information associated with those accounts. The account resets occurred between January and February 2015. Equifax has informed us that the individual is no longer associated with Equifax. The personally identifiable information may have included name, home address, telephone number, social security number, and payroll information.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Rite Aid
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/rite-aid-20150605.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150713-05	National Seating & Mobility	TN	6/15/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

The incident occurred in Atlanta, Georgia on April14, 2015 and involved the theft of two laptops, a smartphone, a backpack, and a briefcase belonging to two NSM employees from the employees' locked work vans. A police report was immediately filed with the local police department and the smartphone was remotely wiped by NSM. Also, promptly after it learned about the theft, NSM initiated an internal review to determine the type of information that was contained on the stolen items.

Attribution 1 Publication: NH AG's office Author:
Article Title: National Seating & Mobility
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/national-seating-and-mobility-20150612.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150713-04	United Seating and Mobility/dba Numotion	CT	6/10/2015	Electronic	Medical/Healthcare	Yes - Published #	2,722

United Seating and Mobility, LLC d/b/a Numotion CT Healthcare Provider 2722 06/10/2015 Theft Laptop

Attribution 1 Publication: hhs.gov / NH AG's office Author:
Article Title: United Seating and Mobility/dba Numotion
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
ITRC20150713-03	CVS Health	RI	6/26/2015	Electronic	Medical/Healthcare	Yes - Published #	12,914

CVS Health RI Healthcare Provider 12914 06/26/2015 Theft Desktop Computer

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150713-02	Service Systems Associates / Zoos	CO	7/9/2015	Electronic	Business	Yes - Published #	60,000

Service Systems Associates, Inc. (SSA) yesterday announced that the point of sale (PoS) systems in the gift shops of several of its clients were recently breached.
"This means that if a guest used a credit or debit card in the gift shop at one of our partner facilities between March 23 and June 25, 2015, the information on that card may have been compromised," company CEO Timothy L. Brantley said in a statement. The data exposed includes customer names, credit or debit card numbers, expiration dates and CVV codes.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: Update: Service Systems Associates breach impacted 60,000
Article URL: http://www.databreaches.net/update-service-systems-associates-breach-impacted-60000/

Attribution 2 Publication: esecurityplanet.com / CA AG's office Author:
Article Title: Nine Zoos Nationwide Suffer Point-of-Sale Breaches
Article URL: http://www.esecurityplanet.com/network-security/nine-zoos-nationwide-suffer-point-of-sale-breaches.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150713-01	New Horizons Computer Learning Centers	CA	7/13/2015	Electronic	Educational	Yes - Unknown #	Unknown

New Horizons Computer Learning Centers, Inc. ("New Horizons") recently discovered an incident that may affect the security of your personal information. We are unaware of any attempted or actual misuse of your personal information, but are providing this notice to ensure that you are aware of the incident so that you can take steps to protect your information.

Attribution 1 Publication: CA AG's office Author:
Article Title: New Horizons Computer Learning Centers
Article URL: https://oag.ca.gov/system/files/New%20Horizons%20notice%20only%207_10_15_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150709-01	Evans Hotels	CA	7/8/2015	Electronic	Business	Yes - Unknown #	Unknown

The operator of three San Diego hotels announced Wednesday that a security breach led to unauthorized charges on guests' payments cards, and recommended that guests review their accounts for the affected time period. Evans Hotels -- which owns and operates the Bahia Resort, Catamaran Resort and The Lodge at Torrey Pines -- received calls in February from guests who saw unauthorized charges on their payments cards after they were used at the company's hotels.

Attribution 1 Publication: sandiego6.com Author:
Article Title: Security breach at 3 local hotels allows unauthorized payments
Article URL: http://www.sandiego6.com/news/local/Security-breach-at-3-local-hotels--312665811.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150707-08	Trump Hotel Properties	NY	7/1/2015	Electronic	Business	Yes - Unknown #	Unknown

The Trump Hotel Collection, a string of luxury hotel properties tied to business magnate and now Republican presidential candidate Donald Trump, appears to be the latest victim of a credit card breach, according to data shared by several U.S.-based banks.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Banks: Card Breach at Trump Hotel Properties
Article URL: http://krebsonsecurity.com/2015/07/banks-card-breach-at-trump-hotel-properties/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150707-07	Harvard University	MA	7/1/2015	Electronic	Educational	Yes - Unknown #	Unknown

Harvard University has discovered an intrusion into its data systems, the school announced Wednesday in an e-mail to staff, faculty, and students. The university discovered the breach in the technology networks of the Faculty of Arts and Sciences and Central Administration on June 19, according to the e-mail from Provost Alan Garber and Katie Lapp, the school's executive vice president.
Security officials do not believe personal data, research data, e-mails, or PIN numbers have been exposed. But it is possible that hackers obtained Harvard login credentials to access individual computers and university e-mail accounts, the e-mail said

Attribution 1 Publication: bostonglobe.com Author:
Article Title: Harvard says data breach occurred in June
Article URL: https://www.bostonglobe.com/metro/2015/07/01/harvard-announces-data-breach/pqzk9IPWLMiCKBl3IijMUJ/story.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150707-06	Firekeepers Casino	MI	7/3/2015	Electronic	Business	Yes - Published #	85,000

Information from thousands of credit and debit cards may have been stolen during a data security breach at FireKeepers Casino in Battle Creek. Officials with FireKeepers Casino confirmed Friday that approximately 85,000 credit and debit cards used between September 7, 2014, and April 25, 2015, for food, beverage and retail purchases may have been affected by the breach.

Attribution 1 Publication: databreaches.net / woodtv.com / NH AG Author:
Article Title: Around 85K affected in FireKeepers Casino data breach
Article URL: http://woodtv.com/2015/07/03/around-85k-affected-in-firekeepers-casino-data-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150707-05	University of California San Francisco	CA	7/4/2015	Electronic	Medical/Healthcare	Yes - Published #	435

UC San Francisco is alerting individuals about a burglary involving an unencrypted laptop belonging to a faculty member in the Cardiac Electrophysiology & Arrhythmia Service that contained some personal, research and health information.

Attribution 1 Publication: databreaches.net Author:
Article Title: Stolen laptop contained UCSF research participants' health & insurance info
Article URL: http://www.databreaches.net/stolen-laptop-contained-ucsf-research-participants-health-insurance-info/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150707-04	**UPMC Health Plan**	PA	7/2/2015	Electronic	Medical/Healthcare	Yes - Published #	**722**

UPMC health plan has reported a data breach affected 722 insurance subscribers. This is the second data breach to affect the health plan this year. In May UPMC reported 2,000 patient records had been compromised. The latest data breach appears to have resulted from an internal error. Yesterday, UPMC spokeswoman, Gina Pferdehirt, said patient information was compromised when an email containing PHI was sent to an unauthorized person.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: UPMC Health Plan
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9165418C0572F90093232617A5E2372D.ajp13w

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150707-03	**Cuesta College**	CA	7/6/2015	Electronic	Educational	Yes - Published #	**4,000**

Cuesta College is offering one year of free identity theft protection to current and former community college employees who were affected by a recent database breach. Paso Robles resident Lacey Fowler, a human resources analyst at Cuesta College, is accused of illegally accessing the college's personnel database May 31, which contained private information about employees.

Attribution 1 Publication: sanluisobispo.com / esecurityplanet.com Author:
Article Title: Cuesta College to offer free ID theft protection after data breach
Article URL: http://www.sanluisobispo.com/2015/07/06/3710702/cuesta-college-id-theft-protection.html

Attribution 2 Publication: esecurityplanet.com Author:
Article Title: Orlando Health, Cuesta College, Firekeepers Casino Acknowledge Data Breaches
Article URL: http://www.esecurityplanet.com/network-security/orlando-health-cuesta-college-firekeepers-casino-acknowledge-data-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150707-02	**Montefiore Health System**	NY	7/6/2015	Electronic	Medical/Healthcare	Yes - Published #	**12,517**

Bronx, N.Y.-based Montefiore Health System received word May 15 from law enforcement that an employee had stolen the personal health information of more than 12,000 patients. Montefiore fired the employee, who has also been arrested and is facing prosecution. Eight others believed to be involved in a "theft ring" related to the crime have been indicted.

Attribution 1 Publication: hipaajournal.com / MD AG's office Author:
Article Title: HIPAA Breach for Handbags: Manhattan DA Indicts 8 in ID Theft Ring
Article URL: http://www.hipaajournal.com/hipaa-breach-for-handbags-manhattan-da-indicts-8-in-id-theft-ring-7091/

Attribution 2 Publication: beckershospitalreview.com Author:
Article Title: Montefiore Health System
Article URL: http://www.beckershospitalreview.com/healthcare-information-technology/9-latest-data-breaches.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150707-01	**Orlando Health**	FL	7/6/2015	Electronic	Medical/Healthcare	Yes - Published #	**3,421**

Orlando (Fla.) Health is notifying patients of a data breach after discovering a nursing assistant had accessed patient records in a manner unrelated to job responsibilities. The health system learned of the inappropriate access to information during a May 27 routine patient record access audit, according to a notice posted on its website. The nursing assistant accessed patients' electronic records, which may have included patient names, birth dates, addresses, medications, medical tests and results, other clinical information and the last four digits of Social Security numbers. Additionally, the employee may have accessed insurance information for "a limited number" of patients, according to the health system.

Attribution 1 Publication: beckershospitalreview.com / hhs.gov Author:
Article Title: Orlando Health reports data breach due to illegal employee access affects 3,200 patients
Article URL: http://www.beckershospitalreview.com/healthcare-information-technology/orlando-health-reports-data-breach-due-to-i

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150706-03	Covanta Projects, LLC	NJ	7/1/2015	Electronic	Business	Yes - Unknown #	Unknown

On behalf of Covanta Projects, LLC (Covanta), I am writing to inform you about an unfortunate incident that occurred and was reported on May 20, 2015. An automobile, belonging to a member of the Human Resources department, was broken into and among the items stolen was a Covanta-issued laptop. Covanta and the authorities were promptly notified and Covanta immediately began an investigation to determine what information was contained on the laptop.

Attribution 1 Publication: VT AG's office Author:
Article Title: Covanta Projects, LLC
Article URL: http://www.ago.vermont.gov/assets/files/Consumer/Security_Breach/2015-06-15%20Covanta%20SBN%20to%20Consu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150706-02	Automotive Recovery Services (Vehicle Donation	IL	7/1/2015	Electronic	Business	Yes - Published #	17,215

ARS takes the security of this information seriously. Unfortunately, we have discovered that unauthorized person(s) gained access to certain VDPC legacy systems. While the source of this intrusion is still under investigation, it may have exposed your personal information between July 2012 and May 2015, including your name, social security number, street address, email address, phone number, drivers license number, the type of vehicle you donated, and/or the name of the charity to which you donated your vehicle. This incident occurred on our systems and not the systems of the charity to which you donated your vehicle. (17,215 = Maryland residents)

Attribution 1 Publication: CA AG's office / VT AG's office Author:
Article Title: Automotive Recovery Services (Vehicle Donation Processing Center)
Article URL: https://oag.ca.gov/system/files/KAR_Sample%20Consumer%20Breach%20Notification%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150706-01	Bonita Unified School District	CA	6/30/2015	Electronic	Educational	Yes - Unknown #	Unknown

On June 2, 2015, we discovered that unauthorized individuals gained access to our student database in May 2015 and changed the grades of several students at San Dimas High School. We believe the suspects also accessed and downloaded personal information relating to students, including your name, Social Security number, birthdate, medical information, Aeris user name and password, and contact information, such as physical address, email address and phone number.

Attribution 1 Publication: CA AG's office Author:
Article Title: Bonita Unified School District
Article URL: https://oag.ca.gov/system/files/BONITAUSD_B1194_BONITA_USD_%20NOTIFICATION_LETTER_STUDENT_ADULT.DO

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150630-02	DK Real Estate MGMT	FL	6/29/2015	Electronic	Business	Yes - Published #	400

A local business had the personal information stolen for hundreds of people, including driver licenses, Social Security numbers and bank records.

Attribution 1 Publication: databreaches.net / winknews.com Author:
Article Title: Personal information stolen for hundreds of people
Article URL: http://www.winknews.com/2015/06/29/personal-information-stolen-for-hundreds-of-people/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150630-01	Advanced Tech Support / Inbound Call Experts	FL	6/29/2015	Electronic	Business	Yes - Unknown #	Unknown

The Florida inbound call center Advanced Tech Support, which is run by Inbound Call Experts, has suffered a insider data breach, IDG News Service reports. In a notice that has since been removed from its website, Advanced Tech Support warned that customers may be targeted by a scam in which callers claim to be Advanced Tech Support representatives, and attempt to gain access to the customer's computer.

Attribution 1 Publication: esecurityplanet.com Author: Jeff Goldman
Article Title: Advanced Tech Support Suffers Insider Breach
Article URL: http://www.esecurityplanet.com/network-security/advanced-tech-support-suffers-insider-breach.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150629-19	Manchester Hotel Hospitality / Six Continents Hotel (IHG)	TN	6/23/2015	Electronic	Business	Yes - Unknown #	Unknown

On February 11, 2015, the Company was contacted by Six Continents Hotels ("IHG"), who was previously notified by the United States Secret Service, that certain hotels affiliated with IHG had been identified as potential victims of a data security incident. It was suggested that the Company conduct a formal investigation into a potential data breach at its hotel location in Manchester, Tennessee. IHG engaged Dell SecureWorks to conduct a forensic investigation, and the report of such investigation was provided to the Company on April 29th, 2015.

Attribution 1 Publication: NH AG's office Author:
Article Title: Six Continents Hotel (IHG) / Manchester Hotel Hospitality
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/manchester-hotel-hospitality-20150623.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150629-18	Genius Central	FL	6/24/2015	Electronic	Business	Yes - Published #	256

GC noticed that part of its network was running slower than normal, and immediately investigated the situation. It was determined that assistance from a forensic computer consultant was prudent. During the investigation, on May 12, 2015, the computer consultant determined that malware was installed on GC's system on or about January 9, 2015, which may have exposed social security information pertaining to 256 individuals.

Attribution 1 Publication: NH AG's office / VT AG's office Author:
Article Title: Genius Central
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/genius-central-20150624.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150629-17	Success 4 Kids & Families, Inc.	FL	5/20/2015	Electronic	Medical/Healthcare	Yes - Published #	506

Success 4 Kids & Families, Inc. FL Healthcare Provider 506 05/20/2015 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Success 4 Kids & Families, 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
ITRC20150629-16	Hershey Entertainment & Resorts Company	PA	6/26/2015	Electronic	Business	Yes - Unknown #	Unknown

The Pennsylvania amusement park Hersheypark is investigating a possible credit card breach, according to KrebsOnSecurity's Brian Krebs. The company has hired a security firm to look into reports from several financial institutions about a pattern of fraud on credit cards used at Hershey properties. Specifically, sources at three financial institutions told Krebs they detected a pattern of fraudulent activity on cards used at Hershey locations, including food and beverage outlets, ticket stations and the Hershey Lodge, between mid-March and late May 2015.

Attribution 1 Publication: esecurityplanet.com Author:
Article Title: Hersheypark Investigates Possible Credit Card Breach
Article URL: http://www.esecurityplanet.com/network-security/hersheypark-investigates-possible-credit-card-breach.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150629-15	Meritus Medical Center	MD	6/27/2015	Electronic	Medical/Healthcare	Yes - Published #	1,029

Meritus Medical Center is contacting patients about a “privacy incident” that may have compromised personal data, including names, demographics, clinical information and Social Security numbers. Meritus mailed out letters Friday to 1,029 individuals who may have been affected after conducting an investigation into the matter, according to a news release and a Meritus spokeswoman.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Meritus Medical Center
Article URL: http://www.databreaches.net/md-meritus-contacting-patients-after-privacy-incident/

Attribution 2 Publication: hhs.gov Author:
Article Title: OCR
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
ITRC20150629-14	County of Lancaster EMS	SC	6/4/2015	Electronic	Government/Military	Yes - Published #	50,000

Sometimes even the best protections are not enough, as Lancaster County, EMS, S.C discovered when a safe used to store unencrypted flash drives securely was discovered to have gone missing. A thorough search of the building was organized but the safe, along with its contents, were nowhere to be found. County officials have stated that they have no reason to believe that the information has been used inappropriately but there is a risk that the safe has been opened and the contents – two flash drives and two computer hard drives – may have been accessed.

Attribution 1 Publication: hipaajournal.com / hhs.gov / beckershos Author:
Article Title: County of Lancaster EMS
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
ITRC20150629-12	Department of Aging and Disability Services	TX	6/11/2015	Electronic	Government/Military	Yes - Published #	6,600

On June 11, the Texas Department of Aging and Disability Services announced that the protected health information of approximately 6,600 Medicaid recipients may have been released unintentionally. The agency stated that a web application intended for internal use only was accessible on the Internet. The application contained patients' names, residences, addresses, birth dates, Social Security numbers, medical diagnoses and treatment information.

Attribution 1 Publication: hhs.gov / beckershospitalreview.com Author:
Article Title: Department of Aging and Disability 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
ITRC20150629-11	St. Martin Parish School-Based Health Centers	LA	6/15/2015	Electronic	Medical/Healthcare	Yes - Published #	3,000

St. Martin Parish School Based Health Centers LA Healthcare Provider 3000 06/15/2015 Theft Desktop Computer, Electronic Medical Record, Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: St. Martin Parish School-Based Health Centers
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
ITRC20150629-10	Central Brooklyn Medical Group, PC	NY	6/19/2015	Electronic	Medical/Healthcare	Yes - Published #	4,223

Central Brooklyn Medical Group, PC NY Healthcare Provider 4223 06/19/2015 Unauthorized Access/DisclosureOther

Attribution 1 Publication: hhs.gov Author:
Article Title: Central Brooklyn Medical Group, 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
ITRC20150629-09	Truman Medical Center	MO	6/9/2015	Electronic	Medical/Healthcare	Yes - Published #	503

Truman Medical Center, Incorporated MO Healthcare Provider 503 06/09/2015 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Truman 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
ITRC20150629-08	**Keystone Pharmacy, Inc.**	MD	6/9/2015	Paper Data	Medical/Healthcare	Yes - Published #	**500**

On April 27, 2015, rioting broke out in Baltimore, MD and the covered entity (CE), Keystone Pharmacy, was broken into, vandalized and looted. Multiple prescriptions and stock bottles of narcotics were taken. About 150 prescription bags containing patient names and the medications were stolen. The types of protected health information (PHI) contained on the prescriptions included names, addresses, and prescription information.

Attribution 1 Publication: hhs.gov / OCR Author:
Article Title: Keystone Pharmacy, 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
ITRC20150629-07	**Implants, Dentures & Dental DBA Half Dental**	NV	6/10/2015	Electronic	Medical/Healthcare	Yes - Published #	**12,000**

Implants, Dentures & Dental DBA Half Dental NV Healthcare Provider 12000 06/10/2015 Theft Electronic Medical Record, Laptop, Network Server, Other, Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: Implants, Dentures & Dental DBA Half Dental
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150629-05	**LC Industries, Inc.**	NC	6/29/2015	Electronic	Business	Yes - Published #	**3,754**

North Carolina-based LC Industries, Inc., which operates the Tactical Assault Gear website, is notifying thousands of customers that malware discovered on the website was being used to gain access to personal information.

Attribution 1 Publication: scmagazine.com / NH AG's office / VT A Author:
Article Title: Malware on Tactical Assault Gear website targets customer information
Article URL: http://www.scmagazine.com/malware-on-tactical-assault-gear-website-targets-customer-information/article/423302/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150629-04	**University of California Irvine Medical Center**	CA	6/19/2015	Electronic	Medical/Healthcare	Yes - Published #	**4,859**

University of California (UC) Irvine Medical Center is notifying nearly 5,000 patients that an employee accessed their records without a job-related purpose between June 2011 and March.

Attribution 1 Publication: scmagazine.com / hhs.gov Author:
Article Title: UC Irvine Medical Center announces breach affecting 4,859 patients
Article URL: http://www.scmagazine.com/uc-irvine-medical-center-announces-breach-affecting-4859-patients/article/421645/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150629-03	**COA Network**	NJ	6/24/2015	Electronic	Business	Yes - Unknown #	**Unknown**

COA Network, Inc. – a New Jersey company that provides virtual telephone systems and content management systems – detected a pattern of irregular activity affecting its computer systems, and is treating all customer information as being potentially compromised. How many victims? All customers are being treated as potentially compromised. What type of personal information? Names, addresses, email addresses, payment card numbers and expiration dates.

Attribution 1 Publication: scmagazine.com / MD AG's office / NH Author:
Article Title: COA Network breached, all customer data treated as potentially compromised
Article URL: http://www.scmagazine.com/coa-network-breached-all-customer-data-treated-as-potentially-compromised/article/4226

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150629-02	**Medical Informatics Engineering (MIE) /**	IN	6/1/2015	Electronic	Medical/Healthcare	Yes - Published #	**3,900,000**

Medical Informatics Engineering ("MIE") is writing to provide notice of a data security compromise that may have affected the security of some protected health information contained on our network, relating to certain [client name] patients. On May 26, 2015, the technical team at MIE discovered suspicious activity relating to one of our servers. While our investigation and law enforcement's investigation into this incident are ongoing, we determined that some protected health information contained on our network relating to a soon to be confined number of patients was exposed as a result of this incident. The affected data may include patient name, home address, email address, date of birth, and for some patients a Social Security number.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Medical Informatics Engineering (MIE)
Article URL: https://oag.ca.gov/system/files/Medical%20Informatics%20notice%20only6_26_15_0_0.pdf?

Attribution 2 Publication: hipaajournal.com Author:
Article Title: Data Breach Sparks Medical Informatics Engineering Lawsuit
Article URL: http://www.hipaajournal.com/data-breach-medical-informatics-engineering-lawsuit-8054/

Attribution 3 Publication: MIE website Author:
Article Title: Medical Informatics Engineering (MIE) / NoMoreClipboard
Article URL: https://www.mieweb.com/notice/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150629-01	**Bank of Manhattan - Mortgage Lending**	CA	6/12/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

We believe in acting quickly to protect our customers' best interests. Thus, we are contacting you to inform you about a recent data security incident at Bank of Manhattan Mortgage Lending. Our investigation is ongoing, but it appears that an employee handled mortgage loan files stored on a removable disk drive in a manner that was contrary to our policies and instructions, and may have resulted in unauthorized disclosure or use of information in those files. These files included a loan that was originated for you at Bank of Manhattan Mortgage Lending, or was owned by Bank of Manhattan Mortgage Lending at one point. The loan files include name, address, loan number, phone numbers, Social Security numbers, birth dates, credit information, tax information, and other financial information.

Attribution 1 Publication: CA AG's office / scmagazine.com Author:
Article Title: Bank of Manhattan - Mortgage Lending
Article URL: https://oag.ca.gov/system/files/Bank%20of%20Manhattan%20Customer%20Notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150625-02	**Summit Financial Group**	TX	6/22/2015	Electronic	Business	Yes - Published #	**Unknown**

After a Summit client files a tax return, we mail the client a CD that contains his or her tax return. Between January I, 2015 and February 15, 2015, in connection with performing tax return services for our clients, we mailed CDs to sixty-seven clients. We intended that these CDs would contain only the individual recipient's tax retum information. On April 15, 2015, a client contacted Summit to inform us that a single CD had other clients' data on it.

Attribution 1 Publication: CA AG's office Author:
Article Title: Summit Financial Group
Article URL: https://oag.ca.gov/system/files/Sample%20Notice%201_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150625-01	**Trustmark Mutual Holding Company**	IL	6/22/2015	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

On May 13, 2015, our automated billing e-mail system generated and sent encrypted e-mails to certain insurance carrier clients. While each encrypted email should have contained a single file with information related to each carrier's insureds, on May 14, 2015, we discovered that a software error resulted in each carrier receiving file attachments for all of the carriers instead of just the one related to their own insureds

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Trustmark Mutual Holding Company
Article URL: https://oag.ca.gov/system/files/Notice%20of%20Event_0.pdf?

Attribution 2 Publication: hipaajournal.com / MD AG's office Author:
Article Title: Ill. Insurer Discovers PHI Disclosure Caused by Software Glitch
Article URL: http://www.hipaajournal.com/ill-insurer-discovers-phi-disclosure-caused-by-software-glitch-8002/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-15	M&T Bank	NY	5/20/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We are writing to let you know about an incident that occurred that may affect you, and to share with you the steps being taken to address it. On Tuesday, April 21, 2015, the documents you completed during a previous visit to the XXXXXX branch to update account ownership on your checking account ending in XXXX were inadvertently faxed to the incorrect number.

Attribution 1 Publication: MD AG's office Author:
Article Title: M&T Bank
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253908.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-14	esurance	CA	5/20/2015	Electronic	Business	Yes - Unknown #	Unknown

An internal audit has revealed that, during the last week of January 2015, an Esurance claims adjuster, in violation of company policy, unmasked the social security number and date of birth from the claims file of one Maryland resident who was not assigned to said claims adjuster at the time of access

Attribution 1 Publication: MD AG's office Author:
Article Title: esurance
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253907.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-13	Citibank	NY	5/20/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On behalf of Citibank, N.A. ("Citi"), I am writing to inform you about events that took place on March 23, 2015 in which linlited personal information maintained by Citi relating to a Maryland resident was improperly accessed by a Citibank employee. As a result of our investigation, this person is no longer working at Citibank.
Specifically, on May 5, 2015 we discovered that the employee had authorized access to customer account records and used that access to attempt to make fraudulent purchases in the customer's name. We determined that the personal information exposed to the employee was the customer's name, address, telephone number, account number, social security number, and date of birth.

Attribution 1 Publication: MD AG's office Author:
Article Title: Citibank
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253788.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-12	M&T Bank	NY	5/13/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 23, 2015, a service provider for M&T Bank supporting Health Savings Accounts (HSA) inadvertently sent an encrypted e-mail to another client of the service provider, which included a report that contained your first and last name, social security number, health savings account number, and email address.

Attribution 1 Publication: MD AG's office Author:
Article Title: M&T Bank
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253787.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-11	Big Idea Entertainment, LLC	TN	5/8/2015	Electronic	Business	Yes - Unknown #	Unknown

On behalf of Big Idea Entertainment, LLC, I am writing to inform you about a recent incident in which personal information relating to Maryland residents was accessed by an unauthorized third party. Specifically, we recently learned that an unauthorized third party compromised VeggieTales.com, a website we own and operate, and accessed the personal information of certain customers including customers' names, addresses, email addresses and payment card information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Big Idea Entertainment, LLC
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253718.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-10	Regions Bank	AL	5/8/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

While monitoring our Online Banking platform, we detected unauthorized access to certain customer accounts. We launched an immediate investigation and notified law enforcement. Pursuant to Md. Code Ann. Comm. Law§ 14-3504(h), we are writing to notify you of the unauthorized access to personal information- specifically, the financial account number -belonging to one of our Maryland customers. No other Maryland customers were impacted by this incident.

Attribution 1 Publication: MD AG's office Author:
Article Title: Regions Bank
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253663.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-09	Marsh & McLennan Companies / Mercer	NY	5/14/2015	Electronic	Business	Yes - Unknown #	Unknown

On April 12, 2015 a Mercer computer was remotely accessed by an unauthorized individual posing as an information technology help-desk technician seeking to assist the user with a purported virus on her computer. Mercer immediately took steps to investigate the matter and on April 17th, 2015 Mercer confirmed that personal data including name and Social Security Number was contained in one of the Saipem files on the Mercer computer.

Attribution 1 Publication: MD AG's office Author:
Article Title: Marsh & McLennan Companies / Mercer
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253707.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-08	Blair & Associates, LLC	NJ	5/13/2015	Electronic	Business	Yes - Unknown #	Unknown

During the recent filing season, Blair & Associates, LLC became aware of the fact that some of its clients received letters from the IRS stating that a personal income tax return had already been submitted using their information. This situation was promptly reported to the IRS, and Blair & Associates, LLC engaged computer forensics experts to analyze its systems and look for any sign of a compromise. On March 30, 2015, these forensics experts identified evidence of a compromise within Blair & Associates, LLC's system.

Attribution 1 Publication: MD AG's office Author:
Article Title: Blair & Associates, LLC
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253539.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-07	First Command Financial Services	CA	5/7/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

A First Command laptop belonging to one of our Financial Advisors was stolen from his car. First Command immediately changed the password; however, the laptop was not encrypted. A police report was filed but the laptop was never located and returned to First Command. We have no evidence that the personal information has been accessed or used for fraudulent purposes.

Attribution 1 Publication: MD AG's office Author:
Article Title: First Command Financial Services
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253554.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-06	ZenPayroll	CA	5/14/2015	Electronic	Business	Yes - Unknown #	Unknown

On April 29, 2015, ZenPayroll discovered that it had been the target of phishing, an illegal attempt to acquire sensitive information that allowed an unauthorized person to access one ZenPayroll email account. This access began on April 28, 2015 and the unauthorized person used the email account to send phishing messages to others on the morning of April 29. You are receiving this notice because the email account that was affected contained personal information about you that your employer had emailed to ZenPayroll when setting up its payroll account.

Attribution 1 Publication: MD AG's office Author:
Article Title: ZenPayroll
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253546.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-05	Cooper University Health Care	NJ	4/24/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

I am following up on the prior notice sent to you on April 20, 2015 advising you that, on Saturday, April 18, 2015, a document containing your social security number and date of birth was inadvertently attached to an e-mail sent to fourteen current members of the Medical Staff who are completing their Medical Staff reapplication process. As the prior notice indicated, as soon as we were notified of the e-mail, we began a process of retrieving the e-mail and it's attachments from those fourteen members.

Attribution 1 Publication: MD AG's office Author:
Article Title: Cooper University Health Care
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253588%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-04	John Hancock Life Insurance Company / Signator Investors	MA	4/28/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 13, 2015, unauthorized third parties, posing as tech support, accessed a business computer at the field office of a representative of Signator Investors via a phishing attack. Upon discovering the phishing scam, on that same day, the representative took steps to secure the affected computer and sought assistance from Signator Investors' Compliance Department to investigate the incident and ensure remediation. The computer was encrypted, but the unauthorized parties were able to bypass the encryption using the authorization they acquired during the remote access phishing scam and had access to the affected computer for more than one hour before the scam was discovered and the remote access session was terminated.

Attribution 1 Publication: MD AG's office Author:
Article Title: John Hancock Life Insurance Company / Signator Investors
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253565.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-03	Gallagher Pool Wealth Management, LLC	OH	4/24/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On April 2, 2015, Gallagher became aware that customer information may have inadvertently been exposed on the Internet. Gallagher immediately began an investigation and learned that a security vulnerability made the contents of a network drive accessible from the Internet. While connected, the documents and information on the drive could be located through a search engine, such as Google. The thumb drive contained customer information, including name, address, phone number, date of birth, Social Security number and information pertaining to the financial accounts managed by or obtained through Gallagher, such as income levels, employment information and asset distribution.

Attribution 1 Publication: MD AG's office Author:
Article Title: Gallagher Pool Wealth Management, LLC
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253570.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-02	NewMarket Health	MD	4/23/2015	Electronic	Business	Yes - Unknown #	Unknown

I am writing to give you notice of a recent data security incident involving our client, NewMarket Health, LLC ("NewMarket"), an online publishing company and merchant, that occurred when an individual or individuals not associated with NewMarket illegally "hacked" into a NewMarket server which was maintined and hosted by a 3rd party. This hacking resulted in the exposure of name, address, and credit card information belonging to a number of NewMarket customers.

Attribution 1 Publication: MD AG's office Author:
Article Title: NewMarket Health
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253666.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150623-01	Dulaney Valley Memorial Gardens	MD	4/10/2015	Electronic	Business	Yes - Unknown #	Unknown

An unauthorized individual was able to access payroll records and replace the bank information of all of our direct deposit employees. When employees did not receive the week's pay in their bank accounts Friday morning, April 3rd, we were alerted at once.

Attribution 1 Publication: MD AG's office Author:
Article Title: Dulaney Valley Memorial Gardens
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253715.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150622-02	Law Enforcement Targets	MN	3/17/2015	Electronic	Business	Yes - Unknown #	Unknown

As a result of a code that was uploaded through our website's host (the "Host"), certain data was transmitted to an unknown source. The compromised information likely included customer names, mailing addresses, credit card numbers, phone numbers, and email addresses. The database does not collect Social Security numbers or Driver's License numbers, and therefore that information would not have been compromised. There is no evidence at this time that usernames or passwords were acquired.

Attribution 1 Publication: MD AG's office Author:
Article Title: Law Enforcement Targets
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-253672.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150622-01	Dungarees, LLC (Lucky Brand)	CA	6/25/2015	Electronic	Business	Yes - Unknown #	Unknown

After a recent migration of our website from one server to another, Dungarees was a victim of an illegal hack from a foreign entity, which may have resulted in a compromise to your credit card or debit card.

Attribution 1 Publication: CA AG's office / MD AG's office Author:
Article Title: Dungarees, LLC (Lucky Brand)
Article URL: https://oag.ca.gov/system/files/DOCS-%231545590-v3-Generic_Consumer_Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150617-02	Fred's Super Dollar Stores (Fred's Inc)	TN	6/16/2015	Electronic	Business	Yes - Unknown #	Unknown

A security breach at a Memphis-based retailer has the company examining their data system. Fred's Super Dollar stores are taking precautions after what appeared to have been hackers who planted malware on the store's checkout systems.

Attribution 1 Publication: myfoxmemphis.com / krebsonsecurity.c Author:
Article Title: Fred's Investigating Possible Security Breach
Article URL: http://www.myfoxmemphis.com/story/29334931/freds-investigating-possible-security-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150617-01	Office of Personnel Management #2 (Standard	DC	6/17/2015	Electronic	Government/Military	Yes - Published #	21,500,000

Regarding the hack of standard personnel records announced last week, two people briefed on the investigation disclosed Friday that as many as 14 million current and former civilian U.S. government employees have had their information exposed to hackers, a far higher figure than the 4 million the Obama administration initially disclosed. (includes 2 million relatives and other associates)

Attribution 1 Publication: abcnews.go.com Author:
Article Title: 22 Million Affected by OPM Hack, Officials Say
Article URL: http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731

Attribution 2 Publication: bigstory.ap.org Author: Ken Dilanian /Ted Bri
Article Title: Officials: Second hack exposed military and intel data
Article URL: http://bigstory.ap.org/article/d842d757851b4a59aca2aecf2f31995a/union-says-all-federal-workers-fell-victim-hackers

Attribution 3 Publication: wired.com Author: Andy Greenberg
Article Title: OPM Now Admits 5.6m Feds' Fingerprints Were Stolen By Hackers
Article URL: http://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/

Attribution 4 Publication: cnn.com Author: Evan Perez / Tom Lo
Article Title: OPM inspector general questioned over hacking report
Article URL: http://www.cnn.com/2015/06/16/politics/opm-hack-ig-testimony/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-11	LastPass	VA	6/16/2015	Electronic	Business	Yes - Unknown #	Unknown

The password management service LastPass recently announced that suspicious activity was "discovered and blocked" on its network on June 12, 2015.
While no LastPass user accounts were accessed and no encrypted user data (stored passwords) was stolen, the company's investigation has determined that LastPass account email addresses, password reminders, server per user salts and authentication hashes were compromised.

Attribution 1 Publication: esecurityplanet.com Author:
Article Title: LastPass Password Manager Hacked
Article URL: http://www.esecurityplanet.com/network-security/lastpass-password-manager-hacked.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-10	Volcano Precision Guided Therapy	CA	6/9/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On May 21st, Volcano sent out an email to specific Volcano employees communicating information about their retirement account. There was a file attached to the email which was sent inadvertently and contained certain personal information applicable to the employees receiving the communication. The attached file contained the individual's name, email address (personal or work depending upon the email provided by the individual), social security number and employee identification number.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Volcano Precision Guided Therapy
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/volcano-20150609.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-09	Santander Bank #1	MA	5/19/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On April 23, 2015, the Santander Bank Fraud Card Detection group discovered susptoous ATM withdrawals that occurred that day. Upon further investigation, it was determined that a magnetic stripe skimming device had been placed on the ATM vestibule door of our branch located at 253 Essex St, Salem, MA. After reviewing the branch's video sur-Veillance footage, it was determined that the device had been placed on the ATM vestibule door on April 14, 2015 and removed April15, 2015. The personal information potentially compromised included the customer's name, card number, card expiration date, card security code, and card PIN number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Santander Bank
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/santander-20150519.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-08	Roundpoint Mortgage Servicing Corporation	NC	6/9/2015	Electronic	Business	Yes - Unknown #	Unknown

This incident involved sending New Hampshire resident's personal information to a non-affiliated third party. The type of information sent included the resident's Round Point loan number, FHA case number, property address and loan terms along with the first and last name of the borrower.

Attribution 1 Publication: NH AG's office Author:
Article Title: Roundpoint Mortgage Servicing Corporation
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/roundpoint-mortgage-servicing-20150609.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-07	National Seating & Mobility	TN	6/12/2015	Electronic	Medical/Healthcare	Yes - Published #	9,627

The incident occurred in Atlanta, Georgia on April 14, 2015 and involved the theft of two laptops, a smartphone, a backpack, and a briefcase belonging to two NSM employees from the employees' locked work vans. A police report was immediately filed with the local police department and the smartphone was remotely wiped by NSM. Also, promptly after it learned about the theft, NSM initiated an internal review to determine the type of information that was contained on the stolen items.

Attribution 1 Publication: NH AG's office / hhs.gov Author:
Article Title: National Seating & Mobility
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/national-seating-and-mobility-20150612.pdf

Attribution 2 Publication: hhs.gov Author:
Article Title: National Seating & Mobility
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
ITRC20150616-06	Monadnock Regional School District	NH	6/5/2015	Electronic	Educational	Yes - Unknown #	Unknown

On April 30111 2015 between the hours of 2330 and 0500 May Ist 2015, a laptop assigned to an employee of the Monadnock Regional School District was stolen from an unsecured vehicle located at the residence of the employee. The employee notified law enforcement upon discovery of the theft. It is believed that this laptop was stolen for the purpose of exchanging for narcotics.

Attribution 1 Publication: NH AG's office Author:
Article Title: Monadnock Regional School District
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/monadnock-regional-20150605.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-05	Intimacy Management Company	GA	6/3/2015	Electronic	Business	Yes - Unknown #	Unknown

We are writing on behalf of our client, Intimacy Management Company ("Intimacy"). On May 5, 2015, Intimacy discovered that its ecommerce server had been compromised by a criminal intruder. As a result, personal information of its U.S. customers who placed or attempted to place an order at myintimacy.com between December 15th, 2014 and April 30th, 2015 may have been misappropriated. Information that may have been obtained included name, address, credit card number, credit card expiry date and the CVV code supplied to Intimacy by customers between December 15, 2014 and April 30, 2015.

Attribution 1 Publication: NH AG's office Author:
Article Title: Intimacy Management Company
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/intimacy-management-20150603.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-04	**Heartland Dental**	IL	6/3/2015	Electronic	Medical/Healthcare	Yes - Published #	**3,197**

I am writing to notify your office that in connection with the implementation of a new Information Technology (IT) monitoring system, Heartland Dental, LLC recently discovered unauthorized attacks on some of its websites. Upon discovery of this intrusion, we took immediate steps to secure the affected part of our computer network by disabling access to the compromised websites and promptly launched an internal investigation to understand the nature and scope of the incident. During our ongoing internal investigation, we determined that these attacks had compromised certain websites from March 31 , 2013 to March 23, 2015, allowing access to databases housing historical data from employment application records. (3,197 = Indiana)

Attribution 1 Publication: NH AG's office / hhs.gov Author:
Article Title: Heartland Dental
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/heartland-dental-20150603.pdf

Attribution 2 Publication: indystar.com Author:
Article Title: Indiana's top 10 data breaches so far this year
Article URL: http://www.indystar.com/story/money/2015/07/18/indianas-top-10-data-breaches-so-far-year/30360027/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-03	**BAE Systems**	NH	6/4/2015	Electronic	Business	Yes - Unknown #	**Unknown**

In 2014, a BAE Systems extranet site was subjected to a network attack. Due to the nature and scope of the attack, BAE Systems provided the Pentagon's Damage Assessment Management Office's (DAMO) with a data set for analysis. In January, the DAMO alerted us that the data set contained at least two files containing sensitive personal information.

Attribution 1 Publication: NH AG's office Author:
Article Title: BAE Systems
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/bae-systems-20150604.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-02	**Town of Brunswick**	ME	5/15/2015	Electronic	Government/Military	Yes - Unknown #	**Unknown**

On April 28, 2015, the Brunswick Police Department discovered that an unredacted copy of its March 2, 2015 police log had been inadvertently sent to four media outlets, one of which published the information online. We immediately took steps to notify the media outlet of this incident and confirm complete removal of this information from its website.

Attribution 1 Publication: NH AG's office Author:
Article Title: http://doj.nh.gov/consumer/security-breaches/documents/brunswick-20150515.pdf
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/brunswick-20150515.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150616-01	**Akorn Inc**	OH	6/4/2015	Electronic	Medical/Healthcare	Yes - Published #	**50,000**

Pursuant to Section 359-C:20 of the Revised Statutes of New Hampshire, I am writing as counsel for Akorn, Inc. to inform you that Akorn has recently learned that four company e-mail accounts were compromised. Kirkland & Ellis was retained to investigate the incident, and while our investigation is ongoing, our work to date indicates that the e-mail compromise occurred over several weekends starting approximately two months ago, though we have not yet determined the ultimate cause of the breach

Attribution 1 Publication: hipaajournal.com / MD AG's office Author:
Article Title: Akorn Database for the Highest Bidder: Hacker Holds Pharma Data Auction
Article URL: http://www.hipaajournal.com/akorn-database-for-highest-bidder-hacker-holds-pharma-data-auction-7088/

Attribution 2 Publication: NH AG's office Author:
Article Title: Akorn Inc
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/akorn-20150604.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150615-03	Holiday Valley Resort	NY	6/12/2015	Electronic	Business	Yes - Unknown #	Unknown

New York-based Holiday Valley Resort announced that malware may have compromised payment cards used at any of the resort's point-of-sale (POS) devices between October 2014 and June.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Payment card breach at Holiday Valley Resort
Article URL: http://www.scmagazine.com/payment-card-breach-at-holiday-valley-resort/article/420490/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150615-02	Global Care Delivery / North Shore-LIJ Health System	NY	6/15/2015	Electronic	Medical/Healthcare	Yes - Published #	18,213

New York-based North Shore-LIJ Health System is notifying roughly 18,000 patients that five laptop computers – four of which contained their personal information – were stolen in September 2014 from the offices of Global Care Delivery (GCD), a Texas-based contractor.

Attribution 1 Publication: databreaches.net Author:
Article Title: Follow-Up: Company involved in NSUH-LIJ breach folded
Article URL: http://www.databreaches.net/follow-up-company-involved-in-nsuh-lij-breach-folded/

Attribution 2 Publication: scmagazine.com / hhs.gov / MD AG's of Author:
Article Title: Contractor laptops stolen, data on thousands of North Shore-LIJ patients at risk
Article URL: http://www.scmagazine.com/contractor-laptops-stolen-data-on-thousands-of-north-shore-lij-patients-at-risk/article/420

Attribution 3 Publication: hhs.gov Author:
Article Title: OCR
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
ITRC20150615-01	San Luis Obispo County Community College District /	CA	6/11/2015	Electronic	Educational	Yes - Unknown #	Unknown

It has come to the attention of the San Luis Obispo County Community College District ("the District") that on May 31, 2015 a District employee gained unauthorized access to the District's employee database containing the personally identifiable information, and without authorization transmitted that information to the employee's private email account. The information included employee names, home address and telephone numbers, email addresses, and social security numbers.

Attribution 1 Publication: CA AG's office Author:
Article Title: San Luis Obispo County Community College District / Cuesta College
Article URL: https://oag.ca.gov/system/files/Letter%20for%20Mailing%20on%20LH_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150611-01	Missing Links Networks, Inc. / eCellar	CA	6/10/2015	Electronic	Business	Yes - Published #	250,000

We sincerely regret to inform you lhat we learned of a possible security Incident Involvlng credit and debit card data. Beginning on May 27, 2015, we began notifying our winery customers that eCellar Systems, our consumer-direct sales platform, had been breached during lhe monlh of April, 2015 by an unknown Intruder. To that end, each of our winery clients will be sending out notice of this event to their customers and it is likely lhat individual consumers may receive a almllar notice from multiple wineries.

Attribution 1 Publication: eCellar FAQ Author:
Article Title: Missing Links Networks, Inc. / eCellar
Article URL: http://www.ecellar1.com/faq/index.php

Attribution 2 Publication: 5/27/2015 Author:
Article Title: Peter Michael Winery
Article URL: https://oag.ca.gov/system/files/PMW%2C%20Notification%20Letter%2C%20%28US%20%2B%20PR%20-%20MA%29%2

Attribution 3 Publication: CA AG's office Author:
Article Title: Rombauer Vineyards
Article URL: https://oag.ca.gov/system/files/eCellars%20Customer%20Letter_0.pdf?

Attribution 4 Publication: CA AG's office Author:
Article Title: Clif Bar Family Winery & Farm, LLC
Article URL: https://oag.ca.gov/system/files/Clif%20Family%20Consumer%20Notification%20Letter_0.pdf?

Attribution 5 Publication: CA AG's office / VT AG's office Author:
Article Title: Multiple Letters provided to the California AG's office
Article URL: https://oag.ca.gov/ecrime/databreach/list

Attribution 6 Publication: NH AG's office Author:
Article Title: Rombauer Vineyards
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/rombauer-vineyards-20150611.pdf

Attribution 7 Publication: Napa Valley Register Author:
Article Title: Cyber-crime hits Napa County wineries
Article URL: http://napavalleyregister.com/news/local/cyber-crime-hits-napa-county-wineries/article_ab21e9ee-4574-58ed-8195-13d

Attribution 8 Publication: CA AG's office Author:
Article Title: Turley Wine Cellars
Article URL: https://oag.ca.gov/system/files/Turley%20Wine%20Cellars%20AG%20notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150609-09	**Rite Aid Corporation**	PA	6/3/2015	Paper Data	Medical/Healthcare	Yes - Published #	**2,345**

As looted prescription drugs flood Baltimore streets, fueling a surge in violence, pharmacy chain Rite Aid warned customers Wednesday that their personal medical information could be on the streets, too.. Store officials said the labels on prescriptions stolen during the late April riots included patient names, addresses and the names of medication, but not other sensitive data such as Social Security numbers or credit card numbers.

Attribution 1 Publication: hhs.gov Author:
Article Title: Personal medical information, prescriptions stolen from Rite Aid stores in Baltimore during April looting.
Article URL: http://www.baltimoresun.com/news/maryland/baltimore-riots/bs-md-rite-aid-statement-20150603-story.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150609-07	**Metropolitan Hospital Center / New York City Health and**	NY	5/18/2015	Electronic	Government/Military	Yes - Published #	**3,957**

By way of background, HHC has implemented an information governance and security program that, among other things, monitors and detects all email communications that contain PHI and other confidential information that are sent outside of HHC's information systems without proper authorization. The incident in question, which occurred on January 15, 2015, was discovered on March 31, 2015 when, in the course of HHC's monitoring of outgoing emails, we identified an email that contained PHI, including yours, which a Metropolitan employee improperly sent from his HHC email account to his personal email account.

Attribution 1 Publication: www.nyc.gov / hhs.gov Author:
Article Title: Metropolitan Hospital Center / New York City Health and Hospitals
Article URL: http://www.nyc.gov/html/hhc/downloads/pdf/20150518-data-breach-metropolitan.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150609-06	**Eataly NY, LLC**	NY	6/5/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Based upon an extensive forensic investigation, it appears that unauthorized individuals installed malicious software designed to capture payment card information on the computer systems used to process payment card transactions at the NYC Marketplace. We believe that the malware could have compromised payment card data (including name, payment card account number, card expiration date, and the CVV security code) of individuals who used a payment card at the NYC Marketplace between January 16, 2015 and April 2, 2015. If you made a payment card transaction at the NYC Marketplace during that timeframe, your payment card information may be at risk.

Attribution 1 Publication: databreaches.net / Eataly.com Author:
Article Title: Eataly payment card breach spanned 3 months; NYC customers offered credit monitoring services
Article URL: http://www.databreaches.net/eataly-payment-card-breach-spanned-3-months-nyc-customers-offered-credit-monitoring

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150609-05	Saint Francis Hospital Gift Shop	OK	6/5/2015	Electronic	Business	Yes - Unknown #	Unknown

On March 20, 2015, Saint Francis discovered that an unauthorized person remotely installed malware on the point-of-sale device in the gift shop at Saint Francis Hospital. The malware was used to search for payment card data that was routed through the point-of-sale device at the gift shop. The investigation revealed that the malware was installed on the device for a short window of time between March 5, 2015 and March 17, 2015. Information from payment cards that may have been captured during this period includes the cardholder's name, card number, expiration date and verification code.

Attribution 1 Publication: databreaches.net Author:
Article Title: Saint Francis Hospital Gift Shop Acts to Block Payment Card Security Incident
Article URL: http://www.databreaches.net/ok-saint-francis-hospital-gift-shop-acts-to-block-payment-card-security-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150609-04	University of Michigan	MI	6/5/2015	Electronic	Educational	Yes - Unknown #	Unknown

Some email accounts of University of Michigan students and staff have been compromised, according to an alert posted on the school's public safety departmental website Thursday. The alert says that more than 150 people on the system have fallen victim to "phishing emails" this week. People who have clicked on the scam emails have revealed personal information such as their names, dates of birth, Social Security numbers and passwords, according to the alert.

Attribution 1 Publication: mlive.com Author:
Article Title: Scammers get personal info from 150 people on U-M email system
Article URL: http://www.mlive.com/news/ann-arbor/index.ssf/2015/06/scammers_get_personal_info_fro.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150609-03	My Fast Lab	IN	6/7/2015	Paper Data	Medical/Healthcare	Yes - Published #	170

Medical tests. Copies of Social Security cards, driver's licenses and health insurance cards. Names, addresses, phone numbers, blood types. Credit card numbers with expiration dates and security codes. The most intimate personal details of dozens of Northwest Indiana residents' lives, carelessly discarded into a dumpster in the back of a Crown Point strip mall where anyone who happened to be walking by could see.

Attribution 1 Publication: databreaches.net / newitimes.com Author:
Article Title: Dumped: Crown Point medical lab leaves patient information exposed
Article URL: http://www.nwitimes.com/business/healthcare/dumped-crown-point-medical-lab-leaves-patient-information-exposed/a

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150609-02	ADP, LLC / ADP TotalSource	NJ	5/18/2015	Electronic	Business	Yes - Unknown #	Unknown

Unfortunately, on April 7th, and May 18th, 2015 an ADP associate inadvertently transferred through encrypted email a report that included your information to trusted human resources professionals at two other ADP clients. Each human resources professional immediately notified ADP and provided assurance that your information was not used or further disclosed, and was deleted. We truly regret any inconvenience this may cause you

Attribution 1 Publication: CA AG's office Author:
Article Title: ADP, LLC
Article URL: https://oag.ca.gov/system/files/Notification%20letter.6%208%202015_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150609-01	**Blue Shield of California / California Physicians' Service**	CA	5/18/2015	Electronic	Medical/Healthcare	Yes - Published #	**843**

Between May 9, 2015 and May 18, 2015, your PHI may have been disclosed to an otherwise authorized user of the secure website that Blue Shield maintains for use by our group health benefit plan administrators and brokers. Authorized users may access the website (the "Website") to manage information about their own health benefit plan members.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
Article Title: Blue Shield of California
Article URL: https://oag.ca.gov/system/files/Sample%20Member%20Notification%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150605-07	**Mid-America Apartment Communities, Inc. (MAA)**	TN	5/20/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

On April 15, 2015, MAA discovered that a former employee had sold certain names and Social Security numbers of both current and former residents and applicants to an undercover agent for federal law enforcement. MAA has no evidence that this employee ever sold information to individuals who actually misused the information. Nonetheless, MAA provided affected individuals with notification of this incident so that they could take steps to protect themselves.

Attribution 1 Publication: NH AG's office Author:
Article Title: Mid-America Apartment Communities, Inc. (MAA)
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/mid-america-apartment-20150520.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150605-05	**Fred Finch Youth Center**	CA	6/5/2015	Electronic	Medical/Healthcare	Yes - Published #	**6,871**

Fred Finch Youth Center (FFYC) is in the process of notifying 6,871 current and former clients and program participants of a potential breach of Protected Health Information (PHI), after discovering a break-in had occurred at one of FFYC's San Diego County locations on the weekend of April 4th, 2015.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Fred Finch Youth Center Notifies Clients Of Potential Breach Of Personal Health Information
Article URL: http://www.databreaches.net/ca-fred-finch-youth-center-notifies-clients-of-potential-breach-of-personal-health-informa

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150605-04	**Hotel Beacon**	NY	6/4/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Hotel Beacon in New York City is notifying an undisclosed number of individuals that the security of its payment card processing systems was compromised by a third-party intruder.

Attribution 1 Publication: SCMagazine.com / NH AG's office Author: Adam Greenberg
Article Title: Hotel Beacon payment card processing systems compromised
Article URL: http://www.scmagazine.com/hotel-beacon-payment-card-processing-systems-compromised/article/418546/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150605-03	**AeroGrow International**	CO	6/3/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Here at AeroGrow International, Inc., we take the security of our customers' information seriously. Unfortunately, like many companies in today's global digital economy, we recently received information suggesting that we may have experienced a data compromise. As a result of this investigation, we learned on May 5, 2015, that a hacker likely used malicious software (malware) to infiltrate our online servers, which are hosted by a leading service provider. Within days of being notified of the hacking event, the cause of the compromise had been eradicated.

Attribution 1 Publication: CA AG's office / MD AG's office Author:
Article Title: AeroGrow International
Article URL: https://oag.ca.gov/system/files/Current%20Notice%20-%20Final%20B%20Letter%20Only_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150605-02	Green Tree Servicing, LLC	CA	6/1/2015	Electronic	Business	Yes - Unknown #	Unknown

I am writing to explain a recent security incident that may involve your personal information. Green Tree Servicing LLC ("Green Tree") has learned that personal information relating to some customers may have been accessible in a security incident involving potential unauthorized access to certain computer applications residing on servers operated on behalf of Green Tree. The personal information that may have been accessible in the incident includes your name, Social Security number or other personal information included on mortgage forms.

Attribution 1
Publication: CA AG's office / MD AG's office Author:
Article Title: Green Tree Servicing, LLC
Article URL: https://oag.ca.gov/system/files/Green%20Tree%20Sample%20Consumer%20Notification%20Letter%20%28general%29

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150605-01	Gallant Risk & Insurance Services, Inc.	CA	6/3/2015	Electronic	Business	Yes - Published #	995

We are writing to inform you of a recent security incident that may have resulted in the disclosure of your personal information. Although we believe misuse of your information is highly unlikely, this letter contains information about steps your can take to protect your information, and resources we are making available to help you. We take the security of your personal information very seriously, and sincerely apologize for any inconvenience this may cause you.

Attribution 1
Publication: CA AG's office / hhs.gov Author:
Article Title: Gallant Risk & Insurance Services, Inc.
Article URL: https://oag.ca.gov/system/files/Gallant%20notice%20only%20_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150604-01	Office of Personnel Management	DC	6/4/2015	Electronic	Government/Military	Yes - Published #	4,200,000

Hackers broke into the U.S. government personnel office and stole identifying information of at least 4 million federal workers. The Department of Homeland Security said in a statement Thursday that at the beginning of May, data from the Office of Personnel Management and the Interior Department was compromised. (Current and former government employees)

Attribution 1
Publication: washingtonpost.com Author:
Article Title: Chinese breach data of 4 million federal workers
Article URL: http://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-offic

Attribution 2
Publication: forbes.com Author: Kate Vinton
Article Title: Federal Union Says OPM Data Breach Hit Every Single Federal Employee
Article URL: http://www.forbes.com/sites/katevinton/2015/06/11/federal-union-says-opm-data-breach-hit-every-single-federal-emplo

Attribution 3
Publication: abcnews.com Author:
Article Title: 22 Million Affected by OPM Hack, Officials Say
Article URL: http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731

Attribution 4
Publication: AP / News.Yahoo.com Author:
Article Title: APNewsBreak: Massive breach of federal personnel data
Article URL: http://news.yahoo.com/us-officials-massive-breach-federal-personnel-data-210302099--politics.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150603-03	Virginia Credit Union	VA	6/2/2015	Electronic	Banking/Credit/Financial	Yes - Published #	2,000

Virginia Credit Union says more than 2,000 cardholders had their information breached and money stolen. The credit union says this is a case of ATM skimming, where fraudsters place a device on ATMs that allows them to gather data and duplicate cards

Attribution 1
Publication: databreaches.net / nbc12.com Author:
Article Title: VA Credit Union reissuing cards and refunds after data breach
Article URL: http://www.nbc12.com/story/29222158/va-credit-union-reissuing-cards-and-refunds-after-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150603-02	Office of W.G. Bostick	FL	6/1/2015	Electronic	Business	Yes - Unknown #	Unknown

A disturbing discovery was uncovered on Saturday in a Bay area dumpster. Pages of documents containing sensitive personal information was found.

Attribution 1 Publication: wtsp.com / databreaches.ent Author:
Article Title: Lawyer throws personal documents in dumpster
Article URL: http://www.wtsp.com/story/news/local/2015/06/01/attorney-admits-to-tossing-clients-documents-in-dumpster/28320499

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150603-01	Roll Global / The Wonderful Company	CA	5/22/2015	Electronic	Business	Yes - Unknown #	Unknown

Roll Global LLC and its affiliated companies (collectively, "Roll") were recently informed of an isolated security incident involving the personal information of certain current and former employees of Roll. Specifically, on February 27, 2015, a password-protected laptop was stolen from the locked car of an employee of Hub International, a third-party service provider engaged by Roll. Local law enforcement was notified, and the ensuing internal investigation revealed that a limited number of social security numbers were among the information on the laptop.

Attribution 1 Publication: CA AG's office Author:
Article Title: Roll Global / The Wonderful Company
Article URL: https://oag.ca.gov/system/files/Roll%20Press%20Release%20re%20Hub%20Incident_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150602-06	Blue Goose Cantina	TX	5/28/2015	Electronic	Business	Yes - Unknown #	Unknown

Last Wednesday evening we received a complaint from one of our guests that unauthorized charges had been made on his son's credit card. Following additional complaints we realized our computer had been hacked. By 2:00 Thursday afternoon, we completely shut down our McKinney computer, called the police and our credit card processing firm and began soliciting advice from experts.

Attribution 1 Publication: databreaches.net Author:
Article Title: Blue Goose Cantina Linked to Credit Card Theft
Article URL: http://www.databreaches.net/tx-blue-goose-cantina-linked-to-credit-card-theft/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150602-05	AFLAC	GA	5/15/2015	Electronic	Medical/Healthcare	Yes - Published #	6,166

Aflac GA Health Plan 6166 05/15/2015 Unauthorized Access/Disclosure Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150602-04	Buffalo Heart Group	NY	5/29/2015	Electronic	Medical/Healthcare	Yes - Published #	567

The Buffalo Heart Group, LLP, a local medical practice, uncovered a serious breach of its computer system that took place in the Spring, 2014 and affected between 500 and 600 of its patients. The recently completed internal investigation indicated insider wrongdoing resulted in the access of certain health information (full name, date of birth, address, telephone number, e-superbills, appointment schedule) by unnamed third parties operating under the direction of a physician then associated with the medical practice and used by the physician to solicit patients in connection with the physician's new employment

Attribution 1 Publication: databreaches.net / wkbw.com / hhs.gov Author:
Article Title: Buffalo Heart Group discovers insider wrongdoing involving patient information
Article URL: http://www.databreaches.net/buffalo-heart-group-discovers-insider-wrongdoing-involving-patient-information/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150602-03	Richmond Radiology	KY	6/1/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A Madison County man says he found thousands of medical records stuffed in a dumpster. Carl Swanger says Saturday he found 65 boxes filled with patient information, including social security and credit card numbers. He says immediately he knew something wasn't right.

Attribution 1 Publication: databreaches.net Author:
Article Title: Medical records from defunct practice found in Richmond dumpster
Article URL: http://www.databreaches.net/ky-medical-records-from-defunct-practice-found-in-richmond-dumpster/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150602-02	New York State Office of Mental Health - Nathan S.	NY	4/10/2015	Electronic	Government/Military	Yes - Published #	563

New York State Office of Mental Health Nathan S. Kline Institute for Psychiatric Research NY Healthcare Provider 563 04/10/2015 Loss Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: New York State Office of Mental Health - Nathan S. Kline Institue for Psychiatric Research
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
ITRC20150602-01	Alexian Brothers Medical Center	IL	5/19/2015	Electronic	Medical/Healthcare	Yes - Published #	632

Alexian Brothers Medical Center IL Healthcare Provider 632 05/19/2015 Unauthorized Access/Disclosure Desktop Computer

Attribution 1 Publication: hhs.gov Author:
Article Title: Alexian Brothers 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
ITRC20150601-01	U.S. HealthWorks / Dignity Health	CA	5/30/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On April 22, 2015, we learned that a laptop issued to one of our employees had been stolen from the employee's vehicle the night before. The theft was immediately reported to law enforcement, and we immediately began an internal investigation. On May 5, 2015, we determined that the employee's laptop was password protected, but it was not encrypted. After conducting a thorough review, we determined that the laptop may have contained files that included your name, address, date of birth, job title and Social Security number. Although we continue to work with law enforcement, at this time, the computer has not been located.

Attribution 1 Publication: CA AG's office / beckershospitalreview.c Author:
Article Title: U.S. HealthWorks
Article URL: https://oag.ca.gov/system/files/USHW%20Letter_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150528-04	Unity Recovery Group	FL	5/26/2015	Electronic	Medical/Healthcare	Yes - Published #	1,000

We have recently learned that your personal information, held by Unity Recovery Group, Inc. and/or its affiliated companies, including Starting Point Detox, LLC, Lakeside Treatment Center, LLC, Changing Tides Transitional Living, LLC, and Unity Recovery Center, Inc. (collectively "Unity"), was improperly disclosed to one or more recovery and/or rehabilitation service providers, unaffiliated with Unity, without your prior written consent.

Attribution 1 Publication: VT AG's office / scmagazine.com Author:
Article Title: Unity Recovery Group
Article URL: http://www.ago.vermont.gov/assets/files/Consumer/Security_Breach/2015-05-26%20Unity%20Recovery%20Group%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150528-03	Copart	IA	3/31/2015	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you of an incident that may have affected information you provided to Copart. On March 31, 2015, we discovered that an unauthorized person gained access to our computer network.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150528-02	Heartland Payment (Payroll Solutions) Systems	CA	5/8/2015	Electronic	Business	Yes - Published #	2,200

Heartland Payment Systems, Inc. ("Heartland"), was notified on May 8, 2015 that your personal information may have been compromised. An incident occurred at our office in Santa Ana, California. Many items, including password protected computers belonging to Heartland were stolen. One of these computers may have stored your Social Security number and/or bank account information processed for your employer.

Attribution 1 Publication: CA AG's office Author:
Article Title: Heartland Payment Systems
Article URL: https://oag.ca.gov/system/files/Heartland%20Payment%20Systems%20Ad%20r1fin_0.pdf?

Attribution 2 Publication: esecurityplanet.com Author: Jeff Goldman
Article Title: Stolen Computers Lead to New Heartland Payment Systems Breach
Article URL: http://www.esecurityplanet.com/network-security/stolen-computers-lead-to-new-heartland-payment-systems-breach.ht

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150528-01	Thomas H. Boyd Memorial Hospital	IL	5/21/2015	Paper Data	Medical/Healthcare	Yes - Published #	8,300

Boyd Hospital in Carrollton, Ill. has potentially violated the HIPAA Security Rule after it failed to remove medical records from an old property before it was sold. A resident of Jerseyville, Edward Crone, purchased an old property – an ambulance shed in Main Street – from the county on March 19, after it had been sitting dormant on the market for over a year. The shed was being used by the hospital as an off-site storage facility.

Attribution 1 Publication: hhs.gov / databreaches.net / hipaajourn Author:
Article Title: Thomas Boyd Hospital: Potential HIPAA Violations; Theft Allegations; No exposed PHI
Article URL: http://www.hipaajournal.com/boyd-hospital-dispute-property-sale-6554/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150527-03	Department of State	FL	5/26/2015	Electronic	Government/Military	Yes - Published #	13,000

For the second time in two months, Gov. Rick Scott's administration has acknowledged it inadvertently released confidential personal data of private citizens, prompting the state to offer free credit monitoring services to protect people from being victims of identity theft.

Attribution 1 Publication: miamiherald.com / databreaches.net Author: Steve Bousquet
Article Title: Florida releases personal data on 13,000 people, issues 'fraud' alert
Article URL: http://www.miamiherald.com/news/politics-government/state-politics/article22395198.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150527-02	Merchant - American Express	NY	1/14/2015	Electronic	Business	Yes - Unknown #	Unknown

We are strongly committed to the security of our Cardmembers' information and strive to let you know about security concerns as soon as possible. A merchant where you used your American Express Card detected unauthorized access to its data files. At this time, we believe the merchant's affected data files included your American Express Card account number, your name and other Card information such as the expiration date. Importantly, your Social Security number was not impacted and our systems have not detected any unauthorized activity on your Card account related to this incident.

Attribution 1 Publication: CA AG's office Author:
Article Title: Merchant - American Express
Article URL: https://oag.ca.gov/system/files/CA%20AG%20C2015010236_Customer%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150527-01	**Internal Revenue Service (IRS)**	DC	5/27/2015	Electronic	Government/Military	Yes - Published #	**334,000**

The IRS announced today that criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts through IRS' "Get Transcript" application. This data included Social Security information, date of birth and street address.

Attribution 1 Publication: Govinfosecurity.com Author:
Article Title: IRS: Hack Much Wider Than First Thought
Article URL: http://www.govinfosecurity.com/irs-hack-much-wider-than-first-thought-a-8479?rf=2015-08-18-eg&mkt_tok=3RkMMJW

Attribution 2 Publication: IRS Author:
Article Title: IRS Statement on the "Get Transcript" Application
Article URL: http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-11	**Institute for Financial Markets**	DC	5/12/2015	Electronic	Business	Yes - Published #	**248**

This letter is to notify you that our business experienced a data breach. At approximately 3 a.m. Friday, May 8, 2015, a hacker entered our site at theifm.org from IP address 188.143.234.93 (Russian Federation) and continued attacking our online shopping cart until approximately 10:15 a.m.

Attribution 1 Publication: NH AG's Author:
Article Title: Institute for Financial Markets
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/institute-financial-markets-20150512.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-10	**Harbor Homes, Inc.**	NH	5/15/2015	Electronic	Business	Yes - Unknown #	**Unknown**

On April 8, 2015, a former employee of Harbor Homes, Inc. ("Harbor Homes") requested that Harbor Homes send a copy of his Form W-2 for 2014 to the former employee's e-mail address. An employee of Harbor Homes mistakenly attached an electronic file containing the Forms W-2 for 2014 for this former employee, as well as other Harbor Homes' employees, to the e-mail sent to the former employee. The Forms W-2 included personal information of the Harbor Homes' employees, including full names, addresses and Social Security Numbers

Attribution 1 Publication: NH AG's office Author:
Article Title: Harbor Homes, Inc.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/harbor-homes-20150515.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-09	**SafeandVaultStore.com**	WA	5/22/2015	Electronic	Business	Yes - Unknown #	**Unknown**

SafeandVaultStore.com is writing to inform you of a potential data security incident that may have resulted in the disclosure of your personal information, including your name, and credit or debit card number. We take the privacy and security of your information very seriously, and sincerely apologize for any concern or inconvenience this may cause you.

Attribution 1 Publication: VT AG's office Author:
Article Title: SafeandVaultStore.com
Article URL: http://www.ago.vermont.gov/assets/files/Consumer/Security_Breach/2015-05-21%20SafeandVaultStore%20SBN%20to

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-08	Diman Regional Vocational Technical High School	MA	5/21/2015	Electronic	Educational	Yes - Unknown #	Unknown

Diman Regional Vocational Technical High School ("Diman") is writing to provide notice of a data security incident that may affect the security of some of your personal information. What happened? On May 4, 2015, an email with an attached spreadsheet containing personal information was inadvertently sent by an employee in Diman's Human Resources Department to all faculty. The email was recalled that same day, but some individuals had already received the email.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Diman Regional Vocational Technical High School
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Diman%20Regional%20Tech%20HS%20SBN%20to%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-07	LifeView	TN	5/15/2015	Electronic	Business	Yes - Unknown #	Unknown

We are contacting you because of a data security incident. which may involve your personal information. Between January I. 2015, and April 18, 2015. an unauthorized user obtained names and credit card information from our payment processing system. Upon discovery. this system was immediately shut down. reviewed. and has since been replaced with a new system having additional security measures.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: LifeView
Article URL: http://www.ago.vermont.gov/assets/files/Consumer/2015-05-18%20Lifeview%20Outdoors%20SBN%20to%20Consumer

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-06	University of Rochester Medical Center	NY	5/22/2015	Electronic	Medical/Healthcare	Yes - Published #	3,403

For the second time this week, we learn that a departing employee took information to their new job. First it was the Jacobi Medical Center case, where the employee's motives were reportedly innocent: she wanted the information in case she ever had to follow-up on work she had done. Now it's the University of Rochester Medical Center, where a departing employee reported similar motives, but her new employer used the information to recruit patients to their practice. Patti Singer reports

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Nurse took patient info to new employer (and no, it's not the Jacobi Medical Center breach)
Article URL: http://www.databreaches.net/ny-nurse-took-patient-info-to-new-employer-and-no-its-not-the-jacobi-medical-center-bre

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-05	Adult Friend Finder	CA	5/26/2015	Electronic	Business	Yes - Unknown #	Unknown

The recent breaches involving the leak of personal data on millions of customers at online hookup site Adult Friend Finder and mobile spyware maker mSpy give extortionists and blackmailers plenty of ammunition with which to ply their trade. And there is some evidence that ne'er-do-wells are actively trading this data and planning to abuse it for financial gain. Within hours after data on tens (if not hundreds) of thousands of mSpy users leaked onto the Deep Web, miscreants on the "Hell" forum (reachable only via Tor) were busy extracting countless Apple iTunes usernames and passwords from the archive.

Attribution 1 Publication: KrebsonSecurity.com Author:
Article Title: Recent Breaches a Boon to Extortionists
Article URL: http://krebsonsecurity.com/2015/05/recent-breaches-a-boon-to-extortionists/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-04	Beacon Health System	IN	5/26/2015	Electronic	Medical/Healthcare	Yes - Published #	306,789

Although there is no evidence of any actual or attempted misuse of personal or protected health information belonging to Beacon Health System ("Beacon") patients, Beacon is notifying the media and affected patients that it was the subject of a sophisticated phishing attack, and that unauthorized individuals gained access to Beacon employee email boxes, which contained the personal and protected health information of some individuals, including patients

Attribution 1 Publication: healthcareinfosecurity.com / hhs.gov Author:
Article Title: Beacon Health Is Latest Hacker Victim
Article URL: http://www.healthcareinfosecurity.com/beacon-health-latest-hacker-victim-a-8263?rf=2015-05-29-eh&mkt_tok=3RkMM

Attribution 2 Publication: databreaches.net Author:
Article Title: Beacon Health System notifies patients after phishing attack
Article URL: http://www.databreaches.net/beacon-health-system-notifies-patients-after-phishing-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-03	**Federal Reserve Bank of St. Louis**	AL	5/26/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

According to investigative reporter Brian Krebs, the Federal Reserve Bank of St. Louis has acknowledged that its domain name servers were hijacked last month by attackers who redirected Web searches and queries for domains run by the St. Louis Fed to phishing sites. As a result, the St. Louis Fed says, the attackers may have accessed the user name and password of anyone who tried to log into research.stlouisfed.org on April 24, 2015. Passwords have been reset in response.

Attribution 1 Publication: esecurityplanet.com Author:
Article Title: Federal Reserve Bank of St. Louis Hit by Cyber Attack
Article URL: http://www.esecurityplanet.com/hackers/federal-reserve-bank-of-st.-louis-hit-by-cyber-attack.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-02	**Blue Spring Partners / finfunmermaid.com**	ID	5/21/2015	Electronic	Business	Yes - Unknown #	**Unknown**

On April 30, 2015, we detected a system intrusion that occurred on April 25, 2015. Your personal information may have been disclosed which included name, address, email and encrypted password. We immediately implemented procedures to protect all data and prevent unauthorized access and requested an investigation with authorities.

Attribution 1 Publication: CA AG'soffice Author:
Article Title: Blue Spring Partners
Article URL: https://oag.ca.gov/system/files/Blue%20Spring%20Partners%20Ad%20r1prf_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150526-01	**CareFirst BlueCross BlueShield**	MD	5/22/2015	Electronic	Medical/Healthcare	Yes - Published #	**1,100,000**

Cyberattack exposes data of 1.1M CareFirst BCBS members. CareFirst BlueCross BlueShield announced Wednesday a cyberattack on its system compromised the data of 1.1 million past and current CareFirst members across the Mid-Atlantic region, where CareFirst is the largest payer, according to Reuters.

Attribution 1 Publication: beckershospitalreview.com / hhs.gov / M Author:
Article Title: CareFirst BlueCross BlueShield
Article URL: http://www.beckershospitalreview.com/hospital-management-administration/week-in-review-8-biggest-healthcare-stor

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-12	**Osram Sylvania**	MA	5/13/2015	Electronic	Business	Yes - Unknown #	**Unknown**

I am writing to inform you that a vendor of OSRAM SYLVANIA Inc. had a security breach that may have resulted in unauthorized access to a computer account containing personal information of a former employee of OSRAM SYLVANIA who resides in New Hampshire.

Attribution 1 Publication: NH AG's office Author:
Article Title: Osram Sylvania
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/osram-sylvania-20150513.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-11	Fort Campbell Federal Credit Union	TN	5/4/2015	Paper Data	Banking/Credit/Financial	Yes - Published #	1,307

On or around April 7, 2015, Credit Union management became aware that a third-party vendor contracted to produce and mail member statements and various other account notices to Credit Union members inadvertently mailed overdraft notices to a number of our members, including notices intended for other Credit Union members. The overdraft notices included the names, mailing addresses, member numbers and account balances. While our Client does not have any indication that the information has been used improperly, the Credit Union is taking prompt, appropriate precautionary actions to notify affected members and to prevent and detect any attempted misuse of member information.

Attribution 1
Publication: NH AG's office Author:
Article Title: Fort Campbell Federal Credit Union
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/fort-campbell-cu-20150504.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-10	BJL Cleaning Corporation d/b/a Champion Cleaning	MA	5/1/2015	Electronic	Business	Yes - Unknown #	Unknown

This is to notify you that your name and Social Security number may have been accessed or acquired by an unauthorized person as the result of a computer "hacking" incident.

Attribution 1
Publication: NH AG's office Author:
Article Title: BJL Cleaning Corporation d/b/a Champion Cleaning
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/bjl-cleaning-20150501.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-09	Florida Department of Health	FL	5/9/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Patients' personal medical records were stolen from an Orange County Health Department employee's car, and WFTV reporter Jeff Deal asked officials what is being done to prevent it from happening again. The employee told investigators he had the records in a lock box in his car trunk, and that someone broke in and took them.

Attribution 1
Publication: WFTV.com / databreaches.net Author:
Article Title: Medical records stolen from Orange County Health Department employee's SUV
Article URL: http://www.wftv.com/news/news/local/medical-records-stolen-orange-county-health-depart/nmCRn/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-08	Tax DRX	NJ	5/12/2015	Paper Data	Business	Yes - Unknown #	Unknown

Another case where records in a storage unit wind up in the wild when the owner falls behind on storage rent. News12 New Jersey reports: Hundreds of old tax documents with personal information on them were found left out in the trash Tuesday in Edison.

Attribution 1
Publication: databreaches.net Author:
Article Title: Personal tax records found in Edison trash
Article URL: http://www.databreaches.net/nj-personal-tax-records-found-in-edison-trash/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-07	UPMC - University of Pittsburgh Medical Center	PA	5/15/2015	Electronic	Medical/Healthcare	Yes - Published #	2,259

Because of a data theft at an outside medical billing company, about 2,200 people treated at various UPMC emergency departments are being notified in writing that their records may have been illegally disclosed by an employee of Medical Management LLC. MML and its affiliates provide billing services to health care providers throughout the United States, including to UPMC's physician group Emergency Resource Management Inc.

Attribution 1
Publication: Author:
Article Title: University of Pittsburgh Medical Center patients victimized by rogue employee of Medical Management 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
ITRC20150519-06	Jersey City Medical Center	NJ	4/17/2015	Electronic	Medical/Healthcare	Yes - Published #	1,447

On February 19, 2015, as part of routine hospital operations, an employee of Jersey City Medical Center accidentally sent an e-mail meant for internal use that included an attached spreadsheet with some patient information to an unintended email recipient. The spreadsheet included patient names, health insurance payors, dates of admission and discharge, a one-word description of the medical service department from which the patient received services, and patient Medical Center account number.

Attribution 1 Publication: hhs.gov / databreaches.net Author:
Article Title: Jersey City Medical Center employee gaffe exposed patients' PHI in e-mail attachment
Article URL: http://www.databreaches.net/jersey-city-medical-center-employee-gaffe-exposed-patients-phi-in-e-mail-attachment/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-05	ADT LLC Group Health & Welfare Plan	FL	4/7/2015	Electronic	Medical/Healthcare	Yes - Published #	3,074

ADT LLC Group Health & Welfare Plan FL Health Plan 3074 04/07/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: ADT LLC Group Health & Welfare Plan
Article URL: http://www.hipaajournal.com/saint-agnes-healthcare-hack-exposes-25000-hipaa-records-5663/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-04	MetroHealth	OH	5/18/2015	Electronic	Medical/Healthcare	Yes - Published #	981

Ohio-based MetroHealth is notifying nearly 1,000 patients that three computers in its Cardiac Cath Lab were infected with malware, and the affected computers contained their personal information.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Three MetroHealth computers infected with malware, patients notified
Article URL: http://www.scmagazine.com/three-metrohealth-computers-infected-with-malware-patients-notified/article/415322/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-03	Bellevue Hospital Center	NY	4/28/2015	Electronic	Medical/Healthcare	Yes - Published #	3,334

Bellevue Hospital Center operator New York City Health and Hospitals Corporation (HHC) is notifying roughly 3,300 patients that their personal information was included in a spreadsheet that was improperly emailed to an unauthorized recipient.

Attribution 1 Publication: hhs.gov / scmagazine.com Author:
Article Title: Thousands of Bellevue Hospital Center patients notified of data breach
Article URL: http://www.scmagazine.com/thousands-of-bellevue-hospital-center-patients-notified-of-data-breach/article/416405/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-02	Jacobi Medical Center	NY	4/28/2015	Electronic	Medical/Healthcare	Yes - Published #	90,060

The New York City Health and Hospitals Corporation (HHC) this week began to notify about 90,000 HHC patients about the possible disclosure of some of their protected health information (PHI) that may have occurred when a former employee at HHC Jacobi Medical Center in the Bronx improperly accessed and transmitted files containing PHI to her personal email account and her email account at her new employer, which is a New York City agency.

Attribution 1 Publication: hhs.gov / databreaches.net Author:
Article Title: Jacobi Medical Center notifies 90,060 patients after employee emailed PHI to her personal account and new email address at
Article URL: http://www.databreaches.net/ny-jacobi-medical-center-notifies-90060-patients-after-employee-emailed-phi-to-her-perso

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150519-01	Eastern Maine Healthcare Systems	ME	4/17/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A physician practice affiliated with Bangor-based Eastern Maine Healthcare Systems has notified 1,200 patients that their email addresses were accidentally exposed, according to a Bangor Daily News report.

Attribution 1 Publication: beckershospitalreview.com Author:
Article Title: Eastern Maine Healthcare Systems exposes 1,200 patients' email addresses
Article URL: http://www.beckershospitalreview.com/healthcare-information-technology/eastern-maine-healthcare-systems-exposes

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150518-08	Medical Management, LLC	ID	5/13/2015	Electronic	Medical/Healthcare	Yes - Published #	20,512

Federal law enforcement authorities informed MML on March 16, 2015 that a call center employee of MML who was authorized to work within MML's billing system copied certain items of personal information from that billing system and disclosed this information to a third party. After being informed by these federal law enforcement authorities, MML performed an extensive investigation and review.

Attribution 1 Publication: databreaches.net / hhs.net Author:
Article Title: Medical Management LLC's insider breach impacts patients of 40 providers (Update1)
Article URL: http://www.databreaches.net/medical-management-llcs-insider-breach-impacts-patients-of-40-providers/

Attribution 2 Publication: VT AG's office Author:
Article Title: Medical Management, LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Medical%20Management%20LLC%20SBN%20to%20Co

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150518-07	Associated Dentists	MN	5/18/2015	Electronic	Medical/Healthcare	Yes - Published #	4,725

Associated Dentists is notifying affected patients of a data security incident that may affect the security of their protected health information. Associated Dentists and investigating authorities are unaware of any attempted or actual misuse of patients' protected health information. Associated Dentists is providing notification to ensure that patients are aware of the incident so that they may take steps to protect their information should they feel it is appropriate to do so. Associated Dentists is providing one free year of identity monitoring and identity restoration services to affected individuals. On Thursday, March 19, 2015, someone entered Associated Dentists' Roseville office location after hours and stole two laptops belonging to two different doctors at the Roseville location. The theft was discovered on Friday, March 20, 2014. One of the stolen laptops was encrypted but the other was only password protected. Upon learning of the burglary, Associated Dentists contacted law enforcement, but the stolen laptops have not been recovered to date.

Attribution 1 Publication: databreaches.net / Associated Dentists Author:
Article Title: Associated Dentists notifying patients after office burglary
Article URL: http://www.databreaches.net/mn-associated-dentists-notifying-patients-after-office-burglary/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150518-06	CEMEX, Inc.	TX	4/27/2015	Electronic	Medical/Healthcare	Yes - Published #	880

CEMEX, Inc. TX Health Plan 880 04/27/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: CEMEX, 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
ITRC20150518-05	Ventura County Health Care Agency	CA	5/1/2015	Electronic	Government/Military	Yes - Published #	1,339

The names and internal account information for slightly more than 1,300 hospital and clinic patients in the Ventura County-run health system could potentially have been leaked in a privacy breach, county officials reported Friday.

Attribution 1 Publication: Ventura County Star Author:
Article Title: County health system reports privacy breach involving 1,300 people
Article URL: http://www.vcstar.com/news/local-news/county-health-system-reports-privacy-breach-involving-1300-people_6373151

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150518-04	Duke LifePoint Conemaugh Memorial Medical Center	PA	5/15/2015	Electronic	Medical/Healthcare	Yes - Published #	2,259

An employee of the covered entity's (CE) business associate (BA), Medical Management, LLC ("MML"), disclosed the demographic information of 1,551 of the CE's patients to outside parties. The protected health information (PHI) involved in the breach included names, dates of birth, and social security numbers. Following the breach, the CE assisted the BA in responding to the breach and notifying affected individuals. Additionally, OCR reviewed the CE's risk analysis to ensure compliance with the Security Rule

Attribution 1 Publication: hhs.gov / OCR Author:
Article Title: Duke LifePoint Conemaugh Memorial 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
ITRC20150518-03	Pennsylvania State University - College of	PA	5/18/2015	Electronic	Educational	Yes - Published #	17,933

In late November 2014, the Federal Bureau oflnvestigation ("FBI") provided a victim notification report to Penn State relating to suspicious cyber activity directed at certain systems and computers in the College of Engineering (the "College"). Penn State immediately launched a comprehensive internal investigation into the FBI's report and retained leading third-party computer forensics experts to assist in the investigation.

Attribution 1 Publication: CA AG's office Author:
Article Title: Pennsylvania State University - College of Engineering
Article URL: https://oag.ca.gov/system/files/Penn%20State%20notice%20only2015.05.18%20Re_PSU_Security_Incident_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150518-02	Honig's Whistlestop Inc.	MI	5/11/2015	Electronic	Business	Yes - Unknown #	Unknown

On April 9, 2015, we confirmed that our website had been breached. The incident involved an outside source hacking into and accessing certain electronic information that is maintained by Honig's Whistle Stop, Inc., located in Ann Arbor, Michigan ("Honig's"). We have determined that the information involved in this incident included customer name, credit or debit card number, card expiration date, CVV, email address, account number, password, billing address and phone number, shipping address, and phone number. This information was in our records due to your purchase of items from Honig's, either by phone or through our website at https://www.honigs.com/.

Attribution 1 Publication: CA AG's office Author:
Article Title: Honig's Whistlestop Inc.
Article URL: https://oag.ca.gov/system/files/Honig%27s%20Consumer%20Notification%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150518-01	Longwood Management Corporation	CA	5/11/2015	Electronic	Business	Yes - Unknown #	Unknown

On February 11, 2015, a Longwood employee's vehicle was burglarized. During the burglary, a password-protected laptop we issued to this employee was stolen. The employee immediately reported the burglary to local law enforcement and to Longwood. Longwood immediately launched an investigation into the incident, including both the security of the laptop and the type of information that may have been stored on or accessible by the laptop, at the time of the theft.

Attribution 1 Publication: CA AG's office / databreaches.net Author:
Article Title: Longwood Management Corporation
Article URL: https://oag.ca.gov/system/files/Longwood%20Notice%20Template_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150507-03	Orlando Health - paper breach	FL	5/6/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

A man contacted Channel 9 and said Orlando Health compromised his son's identity when his son's personal hospital information ended up in a neighborhood driveway. John Henderson said he was upset after getting a letter from Orlando Health that specifically said the patient list was found in a "neighborhood driveway." Henderson said the letter stated the patient list contained names, medical record numbers, account numbers and even diagnoses.

Attribution 1 Publication: databreaches.net Author:
Article Title: Orlando Health patient information allegedly found in neighborhood driveway
Article URL: http://www.wftv.com/news/news/local/orlando-health-patient-information-allegedly-found/nk9zQ/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150507-02	Summit Health, Inc.	PA	5/6/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On March 18, attorneys for Summit Health, Inc. in Pennsylvania notified the Maryland Attorney General's Office that on February 19, the hospital had learned that some of its employees had fallen for a phishing attempt. As a result of the successful phishing, employees' information in the Lawson Employee Self-Service System, used to access payroll and benefits information, may have been accessed by unauthorized individuals. Included in that system was employees' W-2 tax information, including income and Social Security numbers. Dependents' information might also have been accessed.

Attribution 1 Publication: databreaches.net Author:
Article Title: Summit Health, Inc.
Article URL: http://www.databreaches.net/pennsylvania-based-summit-health-joins-ranks-of-those-falling-for-phishing/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150507-01	Cities Service / Six Continents Hotels	US	5/7/2015	Electronic	Business	Yes - Published #	613

Cities Service, LLC ("Cities Service") operates a Holiday Inn Express• & Suites located in Sulphur, Louisiana. We were recently made aware that our payment processing environment was compromised by malware. Based on our review of the situation and an examination of the impacted data, our forensics specialists have indicated that some personal data belonging to you was potentially exposed. This information includes names, addresses and payment card account numbers and expiration dates. More specifically, the investigation indicated that your payment card, with account number ending in <XXXX>, may have been affected.

Attribution 1 Publication: NH AG's office Author:
Article Title: Cities Service (Six Continents Hotels)
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/cities-services-20150429.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150504-05	Columbian Financial Group / Columbian Mutual Life	NY	4/17/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 18, 2015, Columbian discovered that a flash drive containing personal information for certain Columbian policyholders and their beneficiaries had been lost in the mail. Although the information on the flash drive was not encrypted, it was in a format that rendered it difficult to access. It also does not appear that someone opened the mailing and took the flash drive, but rather, that the package was damaged in transit and the flash drive was lost (but this is not confirmed). While Columbian immediately initiated an investigation, which is ongoing, to date we have been unable to locate the drive. We have determined that the flash drive contained certain personal information for its policyholders and their beneficiaries, including their names, Social Security number, address, and bank account information for certain individuals. (5156 = Maryland)

Attribution 1 Publication: databreaches.net / MD AG's office Author: 5/24/2015
Article Title: Columbian Mutual Life Insurance Company reports lost flash drive
Article URL: http://www.databreaches.net/columbian-mutual-life-insurance-company-reports-lost-flash-drive/

Attribution 2 Publication: NH AG's office Author:
Article Title: Columbian Financial Group
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/columbian-financial-group-20150417.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150504-03	**Abercrombie & Fitch**	OH	4/15/2015	Electronic	Business	Yes - Unknown #	**Unknown**

We are writing to inform you of a recent security incident involving Abercrombie & Fitch ("Abercrombie"), headquartered in New Albany, Ohio. Abercrombie has recently learned that some of its employees' accounts on a self-help human resource portal were accessed by another individual using the employees' usemames and passwords.

Attribution 1 Publication: NH AG's office Author:
Article Title: Abercrombie & Fitch
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/abercrombie-fitch-20150415.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150504-02	**Sally Beauty Holdings, Inc.**	TX	5/4/2015	Electronic	Business	Yes - Published #	**62,210**

For the second time in a year, nationwide beauty products chain Sally Beauty Holdings Inc. says it is investigating reports of unusual credit and debit card activity at some of its U.S. stores. Last week, KrebsOnSecurity began hearing from multiple financial institutions about a pattern of fraudulent charges on cards that were all recentlysally used at Sally Beauty locations in various states. (62,210 = Indiana)

Attribution 1 Publication: indystar.com Author:
Article Title: Indiana's top 10 data breaches so far this year
Article URL: http://www.indystar.com/story/money/2015/07/18/indianas-top-10-data-breaches-so-far-year/30360027/

Attribution 2 Publication: KrebsonSecurity.com Author:
Article Title: Sally Beauty Card Breach, Part Deux?
Article URL: https://krebsonsecurity.com/2015/05/sally-beauty-card-breach-part-deux/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150504-01	**Walgreen Co.**	IL	5/1/2015	Paper Data	Medical/Healthcare	Yes - Published #	**1,138**

Walgreen Co. IL Healthcare Provider 1138 05/01/2015 Loss Paper/Films Business Associate Present: No

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150501-04	**Hard Rock Hotel & Casino**	FL	5/1/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Restaurants, bars and retailers in the sprawling Las Vegas Hard Rock Hotel & Casino experienced a data breach that reportedly lasted seven months before it was discovered last month. A breach was confirmed by Hard Rock International (HRI), a company that operates separately from the hotel but was nonetheless alerted to the incident. "We have been made aware of a data breach at the Las Vegas Hard Rock Hotel & Casino, and believe it to be an isolated incident at this time," an HRI representative said in a statement. "We do not share information or financial technology platforms with this property."

Attribution 1 Publication: thehill.com / CA AG's office Author:
Article Title: Hard Rock Hotel & Casino suffered data breach
Article URL: http://thehill.com/policy/cybersecurity/240820-hard-rock-hotel-casino-suffered-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150501-03	**Harbortouch**	PA	5/1/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Last week, Allentown, Pa. based point-of-sale (POS) maker Harbortouch disclosed that a breach involving "a small number" of its restaurant and bar customers were impacted by malicious software that allowed thieves to siphon customer card data from affected merchants. KrebsOnSecurity has recently heard from a major U.S. card issuer that says the company is radically downplaying the scope of the breach, and that the compromise appears to have impacted more than 4,200 Harbortouch customers nationwide.

Attribution 1 Publication: KrebsonSecurity Author: Brian Krebs
Article Title: Harbortouch is Latest POS Vendor Breach
Article URL: https://krebsonsecurity.com/2015/05/harbortouch-is-latest-pos-vendor-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150501-02	University of California Berkeley	CA	4/30/2015	Electronic	Educational	Yes - Published #	550

Students at UC Berkeley were being notified of a data breach that may have exposed social security numbers and other personal information Thursday, according to Cal Officials.

Attribution 1 Publication: sanfrancisco.cbslocal.com / CA AG's offi Author:
Article Title: UC Berkeley Students Notified Of Data Breach Involving Social Security Numbers, Bank Accounts
Article URL: http://sanfrancisco.cbslocal.com/2015/04/30/uc-berkeley-students-notified-of-data-breach-involving-social-security-nu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150501-01	Partners HealthCare / Nantucket Cottage Hospital	MA	4/30/2015	Electronic	Medical/Healthcare	Yes - Published #	3,321

Boston-based nonprofit health care system Partners HealthCare is notifying about 3,300 patients about a security breach. Partners says in November it learned a group of its workers received phishing emails and provided information in response. Phishing emails trick their targets into handing over passwords or clicking on links that install malicious programs.

Attribution 1 Publication: abcnews.go.com Author:
Article Title: Partners HealthCare Notifies 3,300 Patients of Email Breach
Article URL: http://abcnews.go.com/Technology/wireStory/partners-healthcare-notifies-3300-patients-email-breach-30716877

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150430-02	Wellmont Health System	TN	4/30/2015	Paper Data	Medical/Healthcare	Yes - Published #	1,726

On March 1, 2015, exposed medical records from Wellmont Health System were discovered in a recycling bin in Bristol, Tennessee, according to a Wellmont statement. The information of 1,726 Holston Valley patients, including PHI, was found in the bin and contained notes from a nurse who cared for patients who received treatment at Holston Valley Medical Center between 1998 and 2007.

Attribution 1 Publication: healthitsecurity.com / hhs.gov Author:
Article Title: PHI left in public Tenn. recycling bin by health employee
Article URL: http://healthitsecurity.com/2015/04/30/exposed-medical-records-potentially-puts-patients-at-risk/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150430-01	County of Los Angeles+USC Medical Center / Augustus F.	CA	4/30/2015	Paper Data	Government/Military	Yes - Published #	880

Augustus F. Hawkins (Hawkins) Mental Health Center reported that patient records were found in the home of a facility employee, when a search warrant was being served at the residence on April 3, 2015. The search was unrelated to County business, but authorities reportedly found confidential patient information for 900 Hawkins patients in the nurse's home. (www.dhs.lacounty.gov)

Attribution 1 Publication: healthitsecurity.com / hhs.gov Author:
Article Title: Exposed Medical Records Potentially Puts Patients At Risk
Article URL: http://healthitsecurity.com/2015/04/30/exposed-medical-records-potentially-puts-patients-at-risk/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150429-02	Project Vida Health Center	TN	3/27/2015	Electronic	Medical/Healthcare	Yes - Published #	7,700

Project Vida Health Center TX Healthcare Provider 7700 03/27/2015 Theft Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Project Vida Health Center
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=1515648227CD2A479DBB744C8A8F9066.worker1

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150429-01	Oregon's Health CO-OP	OR	4/28/2015	Electronic	Medical/Healthcare	Yes - Published #	14,000

Oregon's Health CO-OP has notified members of a "security incident" involving a stolen laptop that contained member information. On April 3, a password-protected laptop containing CO-OP member and dependent information was stolen, according to a news release. The theft was immediately reported to law enforcement and an investigation is underway.

Attribution 1 Publication: Scmagazine.com / hhs.gov Author: Adam Greenberg
Article Title: Oregon's Health CO-OP laptop stolen, about 15K members notified
Article URL: http://www.scmagazine.com/oregons-health-co-op-laptop-stolen-about-15k-members-notified/article/412536/

Attribution 2 Publication: bizjournals.com Author:
Article Title: Oregon's Health CO-OP: Stolen laptop leads to security breach
Article URL: http://www.bizjournals.com/portland/blog/health-care-inc/2015/04/oregons-health-co-op-stolen-laptop-leads-to.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-14	Community Mercy Health Partners / Springfield	OH	4/24/2015	Electronic	Medical/Healthcare	Yes - Published #	2,000

An individual was accidently sent the invoices of numerous patients of the covered entity (CE) due to human error after guarantor information on an institutional account was inadvertently changed to an individual patient. The protected health information (PHI) involved in the breach included the demographic, financial, and clinical information of 1,999 individuals. The CE provided breach notification to HHS, affected individuals, and the media. To prevent a future similar occurrence, the covered entity re-educated its patient access/registration staff and began revising processes for institutional payers. OCR reviewed the CE's relevant HIPAA policies and procedures and obtained assurances that the CE implemented the corrective actions listed above.

Attribution 1 Publication: databreaches.net / hhs.gov / OCR Author:
Article Title: Springfield Regional Medical Center patients notified of #HIPAA breach due to mailing error
Article URL: http://www.databreaches.net/oh-springfield-regional-medical-center-patients-notified-of-hipaa-breach-due-to-mailing-e

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-13	Griffin Health Services	CT	4/25/2015	Electronic	Medical/Healthcare	Yes - Published #	397

Earlier in 2014, Griffin Health Services Corp., of which Griffin Faculty Physicians is a part, reported that an unauthorized user might have accessed one of its software systems, which houses names, addresses, Social Security numbers, dates of birth and 2012 W-2 statements. Griffin notified 397 current and former employees about the breach.

Attribution 1 Publication: newstime.com / CT AG's office Author:
Article Title: Connecticut state law reveals huge extent of data privacy losses
Article URL: http://www.newstimes.com/local/article/Connecticut-state-law-reveals-huge-extent-of-data-6223768.php

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-12	Merchant - American Express	NY	4/27/2015	Electronic	Business	Yes - Unknown #	Unknown

We are strongly committed to the security of our Cardmembers' information and strive to let you know about security concerns as soon as possible. A merchant where you used your American Express Card detected unauthorized access to its data files. At this time, we believe the merchant's affected data files included your cancelled American Express Card account number, your name and other Card information such as the expiration date. Importantly, your Social Security number was not impacted and our systems have not detected any unauthorized activity on your cancelled Card account related to this incident.

Attribution 1 Publication: CA AG's office Author:
Article Title: Merchant - American Express
Article URL: https://oag.ca.gov/system/files/C2015020110%20CA%20AG%20-%20Customer%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-11	Stater Brothers	CA	4/8/2015	Electronic	Business	Yes - Unknown #	Unknown

In cooperation with the West Covina Police Department, Stater Bros. Markets requests the public's help in apprehending three suspects who placed a skimmer device on a pin pad in the deli department at a Stater Bros. Supermarket located at 375 North Azusa Avenue in West Covina. An in-store camera captured the photographs of the suspects, See the images of the suspects below. Stater Bros. takes seriously the security of payment card information. Regrettably, on April 8, 2015, we discovered that three suspects connected a small data capture device to the pin pad of a point-of-sale terminal in the deli area of our West Covina, California store.

Attribution 1 Publication: CA AG's office Author:
Article Title: Stater Brothers
Article URL: https://oag.ca.gov/system/files/Staters%20Bros%20-%20Pin%20Pad%20Incident%20Website%20Notice%20v2_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-10	Compass Group USA / NEXTEP	CA	4/27/2015	Electronic	Business	Yes - Unknown #	Unknown

We are providing this notice as a precaution to tell kiosk users about the incident and to call their attention to some steps they may take to help protect themselves.
Based upon an extensive forensic investigation, it appears that unauthorized individuals installed malicious software designed to capture payment card information on certain NEXTEP self-serve kiosks, including those in use at the locations identified above. Your payment card information (including name, payment card account number, card expiration date and the CVV security code) may be at risk if you used a payment card at a NEXTEP self-service kiosk at one of the on-site dining locations identified above between February 2, 2015 and March 9, 2015.

Attribution 1 Publication: CA AG's office Author:
Article Title: Compass Group USA
Article URL: https://oag.ca.gov/system/files/Compass_Proof%20Copy%20Media%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-09	Consolidated Tribal Health Project	CA	4/28/2015	Electronic	Medical/Healthcare	Yes - Published #	4,885

Consolidated Tribal Health Project, Inc. ("CTHP") is writing to notify you of a data security event that may affect certain information relating to you. While we are unaware of any actual or attempted misuse of this information, this letter contains information about the incident and our response, steps you can take to protect your information, and resources we are making available to help you.
What happened? CTHP has become aware of a data security event involving unauthorized access by a former employee to certain CTHP systems and information maintained by CTHP

Attribution 1 Publication: CA AG's office / CTHP press release / h Author:
Article Title: Consolidated Tribal Health Project
Article URL: http://www.databreaches.net/consolidated-tribal-health-project-inc-notifies-employees-and-patients-of-a-data-security-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-08	University of Illinois at Chicago	IL	4/28/2015	Electronic	Medical/Healthcare	Yes - Published #	3,000

A physician's assigned laptop computer containing the electronic protected health information (ePHI) of approximately 3,000 individuals was stolen. The type of ePHI involved in the breach included diagnoses and conditions of the individuals. The covered entity (CE) provided breach notification to HHS, affected individuals, and the media. Following the breach, the CE updated relevant HIPAA policies, including encryption, to ensure the safeguarding of ePHI and sanctioned the physician involved. OCR obtained assurances that the CE implemented the corrective actions listed above. The CE also notified the deans and directors of all the CE's healthcare components of the corrective actions taken in response to this incident.

Attribution 1 Publication: hhs.gov / OCR Author:
Article Title: University of Illinois at Chicago
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
ITRC20150428-07	CompuNet Clinical Laboratories	OH	4/23/2015	Paper Data	Medical/Healthcare	Yes - Published #	2,584

CompuNet Clinical Laboratories OH Healthcare Provider 2584 04/23/2015 LossPaper/Films No

Attribution 1 Publication: hhs.com Author:
Article Title: CompuNet Clinical Laboratories
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
ITRC20150428-06	**Seton Family of Hospitals / Ascension**	TX	4/25/2015	Electronic	Medical/Healthcare	Yes - Published #	**39,000**

Seton Family of Hospitals will provide free identity monitoring and protection services for patients who had their personal information leaked in a phishing attack targeting employee emails. Approximately 39,000 patients received letters about the breach in which hackers accessed protected patient information, including demographic information, medical record numbers, insurance information and Social Security numbers. Seton was notified of the breach on Feb. 26.

Attribution 1 Publication: kxan.com / databreaches.net Author:
Article Title: Seton data breach may affect 39,000 patients
Article URL: http://kxan.com/2015/04/24/39000-affected-in-seton-phishing-attack-targeting-company-emails/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-05	**Community Health Network**	IN	3/20/2015	Paper Data	Medical/Healthcare	Yes - Published #	**650**

Hundreds of patients' test results went missing last month from a Community Health Network office, the hospital network announced Friday. In February, the staff at Physician Network Practice, located in the 2000 block of North Shadeland Avenue, noticed a binder with results had disappeared.

Attribution 1 Publication: databreaches.net hhs.gov Author:
Article Title: Community Health Network patient test results missing
Article URL: http://www.databreaches.net/community-health-network-patient-test-results-missing/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-04	**SolarCity Corporation / TrueNorth Compliance, Inc.**	TX	3/23/2015	Electronic	Business	Yes - Unknown #	**Unknown**

On approximately March 2, 2015, TrueNorth Compliance, Inc. (TrueNorth), a service provider to SolarCity Corporation, discovered that a document containing your information was captured by a search engine web crawler and stored in a cache (temporary storage) on the Internet from February 27, 2015 to March 2, 2015. We are sending you this letter as a cautionary measure because we believe that certain information about you, which may have included your name, Social Security number, date of birth, address and email address may have been available through Google's Internet search engine.

Attribution 1 Publication: MD AG's office Author:
Article Title: SolarCity Corporation / TrueNorth Compliance, Inc.
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-252135%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-03	**BB&T Mortgage Servicing**	NC	3/13/2015	Paper Data	Banking/Credit/Financial	Yes - Published #	**2,846**

In January of this year, BB&T Mortgage Servicing provided the United States Postal Service (USPS) with 2014 Form 1098 Mortgage Interest Statements for delivery to BB&T clients. Shortly thereafter, a BB&T Client Service Supervisor suspected the mailing may have been processed incorrectly when one envelope was returned by an uninterested third party who had received it in error. After an internal investigation, we determined that incomplete mailing addresses were printed on each envelope provided to the USPS. This error caused the coborrower's name, if there was one, to appear on the face of the envelope instead of the street address field. (2,846 = Maryland only)

Attribution 1 Publication: MD AG's office Author:
Article Title: BB&T Mortgage Servicing
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-252018.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-02	**Equity Trust Company**	OH	3/5/2015	Electronic	Banking/Credit/Financial	Yes - Published #	**3,636**

We are contacting you regarding a data security incident at Equity Trust Company ("Equity Trust"). The data security incident, which is more fully described below, began on January 1, 2015, and was discovered by Equity Trust on February 6, 2015. Our investigation has determined that the data security incident affected 3,636 individuals residing in all 50 states. All affected individuals are Individual Retirement Account ("IRA") holders at brokerages supported by Equity Trust's directed trustee services. The data security incident affects 63 individuals who reside in Maryland.

Attribution 1 Publication: MD AG's office Author:
Article Title: Equity Trust Company
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-251957.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150428-01	**Saint Agnes Health Care, Inc. (Ascension)**	MD	4/24/2015	Electronic	Medical/Healthcare	Yes - Published #	**24,967**

Hackers accessed personal information of about 25,000 patients at Saint Agnes Health Care Inc. The breach resulted from an email phishing incident that targeted employee email accounts to access protected health information. The Baltimore health system on Monday said it sent letters to 25,000 individuals notifying them of the incident, which compromised at least one of the following personal details: name, date of birth, gender, medical record number, insurance information and limited clinical information. In four cases, patients' social security numbers were accessed.

Attribution 1 Publication: hhs.gov / bizjournals.com Author: Sarah Gantz
Article Title: Saint Agnes security breach affects 25,000 people
Article URL: http://www.bizjournals.com/baltimore/news/2015/04/27/saint-agnes-security-breach-affects-25-000-people.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150423-03	**St. Vincent Medical Group**	IN	4/22/2015	Electronic	Medical/Healthcare	Yes - Published #	**760**

St. Vincent Medical Group in Indiana, a member of Ascension Health, has provided a substitute notice following an e-mail phishing incident. According to their notice, a copy of which is posted on their web site, on December 14, 2014, they learned that an employee's user name and password had been compromised as a result of e-mail phishing. St.Vincent Medical Group immediately shut down the user name and password of the impacted account and launched an investigation into the matter.

Attribution 1 Publication: databreaches.net Author:
Article Title: St. Vincent Medical Group notifies patients after successful phishing attempt compromises PHI
Article URL: http://www.databreaches.net/in-st-vincent-medical-group-notifies-patients-after-successful-phishing-attempt-compro

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150423-02	**Freedom Smokes, Inc.**	AL	3/16/2015	Electronic	Business	Yes - Unknown #	**Unknown**

We are contacting you as a precautionary measure to let you know about a data security incident that might affect your customer information. We identified that between approximately February 11, 2015 and March 16, 2015, electronic data may have been improperly obtained through unauthorized access to the website for MyFreedomSmokes ("MFS"). Specifically, on March 16, 2015, we discovered unauthorized code on the website and, although the code was encrypted, we believe that this code may have been used to obtain customer data as customers entered the information into the site's shopping cart while making a purchase on the website.

Attribution 1 Publication: CA AG's office Author:
Article Title: Freedom Smokes, Inc.
Article URL: https://oag.ca.gov/system/files/Notice%20to%20CA%20Consumers_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150423-01	**AT&T**	AL	4/23/2015	Electronic	Business	Yes - Unknown #	**Unknown**

AT&T's commitments to customer privacy and data security are top priorities, and we take those commitments very seriously. As part of an ongoing investigation, we determined that your account was accessed without authorization in violation of AT&T's privacy and security policies between February and July, 2014.

Attribution 1 Publication: CA AG's office Author:
Article Title: AT&T
Article URL: https://oag.ca.gov/system/files/CS_California_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150421-02	VA Long Beach Healthcare System	CA	4/20/2015	Paper Data	Government/Military	Yes - Unknown #	Unknown

Documents containing the personal information of veterans seeking treatment at the Veterans Affairs Long Beach Hospital may have been improperly disposed, Veterans Affairs officials said. Army veteran and hospital patient Paulnhu Nguyen said he found a large stack of patient records containing personal information, such as social security numbers, date of births and full names, in a dumpster by the hospital after his appointment on Thursday.

Attribution 1 Publication: abc7.com / databreaches.net Author:
Article Title: VA Long Beach Hospital may have improperly disposed patients' personal information
Article URL: http://abc7.com/news/va-long-beach-hospital-may-have-improperly-disposed-patient-docs/671192/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150421-01	CDC/NIOSH World Trade Center Health Program	GA	4/2/2015	Paper Data	Government/Military	Yes - Published #	958

CDC/NIOSH World Trade Center Health Program (WTCHP) GA Health Plan 958 04/02/2015 Unauthorized Access/DisclosurePaper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: CDC/NIOSH World Trade Center Health Program
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
ITRC20150420-03	Department of Children and Families / Department of	FL	4/17/2015	Electronic	Government/Military	Yes - Published #	200,000

A state employee is behind bars after accessing the personal information of thousands of Floridians. According to the Department of Economic Opportunity, one of their employees managed to access the Florida Department of Children and Families' Florida ACCESS system. He then obtained the names and social security numbers of more than 200,000 people in the DCF system.

Attribution 1 Publication: news4jax.com Author:
Article Title: DCF suffers major security breach
Article URL: http://www.news4jax.com/news/dcf-suffers-major-security-breach/32434532?view=print

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150420-02	Office of Dr. Anthony T.R. Green	NY	3/11/2015	Paper Data	Medical/Healthcare	Yes - Published #	7,448

Dr. Anthony T. R. Green DDS NY Healthcare Provider 7448 03/11/2015 Unauthorized Access/Disclosure Other, Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Dr. Anthony T.R. Green
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
ITRC20150417-01	Howe Riley & Howe PLLC	NH	4/8/2015	Electronic	Business	Yes - Unknown #	Unknown

On April 2, 20 !5, information was inadvertently entered by HRH onto a website HRH believed to be affiliated with the Internal Revenue Service ("IRS"). The information disclosed included the name, business address, phone number, email address and Social Security number of a HRH client. We have been in contact with the company that runs the website and received written confirmation from them that the information will be discarded.

Attribution 1 Publication: NH AG's office Author:
Article Title: Howe Riley & Howe PLLC
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/howe-riley-howe-20150408.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150416-03	American Sleep Medicine	CA	4/16/2015	Electronic	Medical/Healthcare	Yes - Published #	1,787

On March 3, 2015, we discovered an external hard drive had been stolen from a locked server room. After extensively searching the premises, the incident was reported to the San Diego Police Department (Case number #15-012876). [1,787 per hhs.gov list)

Attribution 1 Publication: CA AG's office Author:
Article Title: American Sleep Medicine
Article URL: https://oag.ca.gov/system/files/San%20Diego%20Patient%20Breach%20Notification%20Letter_0.pdf?

Attribution 2 Publication: databreaches.net Author:
Article Title: American Sleep Medicine patients notified of stolen hard drive
Article URL: http://www.databreaches.net/american-sleep-medicine-patients-notified-of-stolen-hard-drive/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150416-02	Children's Heart Center	NV	4/3/2015	Electronic	Medical/Healthcare	Yes - Published #	8,791

Children's Heart Center NV Healthcare Provider 8791 04/03/2015 Unauthorized Access/Disclosure Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: Children's Heart 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
ITRC20150416-01	Allina Health	MN	4/6/2015	Paper Data	Medical/Healthcare	Yes - Published #	6,000

UPDATE: The Minneapolis Isles clinic run by Allina Health System has notified approximately 6,000 patients of a breach of their Protected Health Information (PHI). The clinic discovered instances of improper PHI disposal had occurred after documents containing sensitive information were found in regular trash. HIPAA rules require all documents containing PHI to be rendered unreadable, indecipherable, and incapable of being reconstructed prior to disposal.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: ALLINA HEALTH SYSTEM ALERTS 6,000 ABOUT IMPROPER PHI DISPOSAL
Article URL: http://www.hipaajournal.com/allina-health-system-alerts-6000-about-improper-phi-disposal-8235/

Attribution 2 Publication: hhs.gov / hipaajournal,com Author:
Article Title: Allina Health
Article URL: http://www.hipaajournal.com/allina-health-system-alerts-6000-about-improper-phi-disposal-8235/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150414-04	Schaeffler Group USA	SC	4/2/2015	Electronic	Medical/Healthcare	Yes - Published #	550

Schaeffler Group USA SC Health Plan 550 04/02/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Schaeffler Group USA
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
ITRC20150414-03	Western Montana Clinic	MT	4/2/2015	Electronic	Medical/Healthcare	Yes - Published #	7,038

Western Montana Clinic MT Healthcare Provider 7038 04/02/2015 Hacking/IT Incident Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Western Montana Clinic
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
ITRC20150414-02	Stanislaus Surgical Hospital	CA	4/5/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

We are contacting you regarding a data security incident that occurred on April 5, 2015 at Stanislaus Surgical Hospital's 1501 Oakdale Road building. This incident may potentially expose some of your personal information to others (i.e. your name, address, account number, Social Security number, and other identifying information may have been among the items breached).

Attribution 1 Publication: CA AG's office Author:
Article Title: Stanislaus Surgical Hospital
Article URL: https://oag.ca.gov/system/files/Stanilslaus%20Surgical%20Hospital_041415_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150414-01	Sweaty Bands	OH	4/10/2015	Electronic	Business	Yes - Unknown #	Unknown

On March 18, 2015, we learned that an unauthorized person gained access to the servers hosting our website's payment processing software and installed malicious code on our systems that was able to access customers' personal information. That information was your name, address, telephone number, credit card number, expiration date, and
verification code

Attribution 1 Publication: VT AG's office Author:
Article Title: Sweaty Bands
Article URL: http://www.ago.vermont.gov/assets/files/Consumer/Sweaty%20Bands%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-17	Roxbury Community College	MA	4/10/2015	Electronic	Educational	Yes - Unknown #	Unknown

The attorney general's office is investigating a data breach at Roxbury Community College, the school's president said in an e-mail to the college community on Thursday. President Valerie Roberson did not disclose the nature of the breach, which was discovered around March 16. It was reported to the board of trustees, the state Department of Higher Education and Attorney General Maura Healy's office, Roberson said. Authorities went to the campus Thursday morning to collect evidence and to interview college employees as part of an ongoing investigation.

Attribution 1 Publication: bostonglobe.com / databreaches.net Author:
Article Title: Data breach reported at Roxbury Community College
Article URL: https://www.bostonglobe.com/metro/2015/04/09/data-breach-reported-roxbury-community-college/PMuDBgvc6sm4wqj

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-16	Denton County Health Department	TX	4/10/2015	Electronic	Government/Military	Yes - Published #	874

On February 13, 2015, a Denton County Health Department employee temporarily left a USB drive at a local printing store in order to print a personal document from the device. Unfortunately, that USB drive included 874 unsecured data files of tuberculosis (TB) clinic patients belonging to the Denton County Health Department, including patient names, dates of birth, addresses, TB test results and other protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA). The data files did not include any financial information or any social security numbers.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Denton County Health Department Alerts TB Clinic Patients to Breach
Article URL: http://www.databreaches.net/tx-denton-county-health-department-alerts-tb-clinic-patients-to-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-15	Walter McCann Fanska	KS	4/10/2015	Electronic	Business	Yes - Unknown #	Unknown

Kansas City-based accounting firm Walters McCann Fanska is notifying clients that their personal and financial account information may have been acquired by a hacker or hackers who had access to the firm's network from sometime late last year until late February 2015. To their credit, the firm noticed suspicious activity with some accounts at the end of the February and brought in a forensic investigator, who confirmed on March 4 that there had been a compromise.

Attribution 1 Publication: VT AG's office Author:
Article Title: Walters McCann Fanska notifies clients of network security breach
Article URL: http://www.databreaches.net/walters-mccann-fanska-notifies-clients-of-network-security-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-14	Office of Dr. Patrick Le	CA	4/11/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Christine O'Donnell reports that hundreds of dental records with patients' addresses, insurance information, Social Security numbers, dates of birth, and drivers license numbers were found in what appears to be a vacant building in Orange. Of concern, the building has broken windows and homeless people have been observed going in and out of it for a while now. Fox11's investigation reportedly found that a dentist named Patrick Le owns the building, and it is also his name that appears on the dental records.

Attribution 1 Publication: databreaches.net Author:
Article Title: Hundreds Of Dental Records Found In Vacant Building
Article URL: http://www.databreaches.net/ca-hundreds-of-dental-records-found-in-vacant-building/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-13	Buchanan & Edwards	VA	4/10/2015	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you about an incident involving your personal information. While investigating an incident in which an unauthorized third party unsuccessfully attempted to transfer funds from a Buchanan & Edwards, Inc. ("Buchanan") bahk account, we discovered on March 11, 2015, that an employee's email account had been compromised on or about February 10, 2015. We promptly reset all user passwords and are enhancing our log in requirements and network security to prevent a similar incident from occurring in the future.

Attribution 1 Publication: VT AG's office Author:
Article Title: Buchanan & Edwards
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Buchanan%20and%20Edwards%20SBN%20to%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-11	University of New Hampshire	NH	4/10/2015	Electronic	Educational	Yes - Unknown #	Unknown

On March 16, 2015, the University of New Hampshire learned that the computer of a faculty member may have been accessed by an unauthorized non-UNH agent. That computer contained data files – since removed from the computer - for a limited number of student class records. Those records included social security numbers, which were formerly used as the student identifier at UNH. While we cannot determine conclusively that the files were viewed or copied, the university is providing you with this notification in accordance with New Hampshire law, RSA 359: C-20 "Notice of Security Breach."

Attribution 1 Publication: NH AG's office Author:
Article Title: University of New Hampshire
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/unh-20150410.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-10	Biggby Coffee	MI	4/10/2015	Electronic	Business	Yes - Unknown #	Unknown

Michigan-based Biggby Coffee announced that an intruder forced their way into its systems and accessed a database containing personal information. How many victims? Undisclosed. What type of personal information? Names, addresses, phone numbers, email addresses, and information regarding employment history.

Attribution 1 Publication: SC Magazine Author:
Article Title: Biggby Coffee announces website intrusion, access gained to database
Article URL: http://www.scmagazine.com/biggby-coffee-announces-website-intrusion-access-gained-to-database/article/408510/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-09	HSBC Finance Corporation	NY	3/27/2015	Electronic	Banking/Credit/Financial	Yes - Published #	3,192

At HSBC, we value your business and respect the privacy of your information, which is why we are writing to let you know about a data security incident that involves your personal information. We recently became aware of an incident where personal information about certain customer mortgage accounts was inadvertently made accessible via the Internet which we believe was towards the end of last year. The information available included your name, Social Security number, account number and some old account information, and may have included your phone number. (685 in New Hampshire and 2,507 = Indiana)

Attribution 1 Publication: indystar.com Author:
Article Title: Indiana's top 10 data breaches so far this year
Article URL: http://www.indystar.com/story/money/2015/07/18/indianas-top-10-data-breaches-so-far-year/30360027/

Attribution 2 Publication: CA AG's office / Scmagazine.com Author:
Article Title: HSBC Finance Corporation
Article URL: https://oag.ca.gov/system/files/IdGrd_1%20-%2047%20State%20B_AG_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-08	Homebridge (In-Home Supportive Services)	CA	3/13/2015	Electronic	Business	Yes - Unknown #	Unknown

Homebridge, formerly the In-Home Supportive Services ("IHSS") Consortium, is writing to notify you of a data security incident that may have resulted in the compromise of the personal information of certain current and former Homebridge employees. Homebridge has discovered that cyber criminals deployed malicious software, or "malware," on a limited number of Homebridge computers, which may have allowed the criminals to obtain unauthorized access to certain human resource ("HR") records.

Attribution 1 Publication: CA AG's office Author:
Article Title: Homebridge (In-Home Supportive Services)
Article URL: https://oag.ca.gov/system/files/Homebridge%20Data%20Security%20EE%20Notification%20Letter%2013%20April%202

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-07	Kellogg & Andelson Global Management	CA	4/10/2015	Electronic	Business	Yes - Unknown #	Unknown

We regret to inform you that Kellogg & Andelson Global Management (K&A) recently was the victim of a criminal attach on its computer network. We are sending you this letter because, unfortunately, some of the personal information you have shared with us may have been accessed during that criminal attach. In late February, K&A noticed suspicious activity involving a handful of client accounts. K&A immediately retained a private forensic investigator, who discovered on March 4, 2015 that K&A had suffered a criminal cyber-attack.

Attribution 1 Publication: CA AG's office Author:
Article Title: Kellogg & Andelson Global Management
Article URL: https://oag.ca.gov/system/files/K-A%20Notification%20Letter%20K-A%20Version_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-06	Pediatric Associates	FL	3/24/2015	Paper Data	Medical/Healthcare	Yes - Published #	627

Pediatric Associates FL Healthcare Provider 627 03/24/2015 Loss Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Pediatric 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
ITRC20150413-05	VA Eastern Colorado Health Care System	CO	4/2/2015	Electronic	Government/Military	Yes - Published #	508

VA Eastern Colorado Health Care System(ECHCS) CO Healthcare Provider 508 04/02/2015 Unauthorized Access/Disclosure Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150413-04	Cigna-Health Spring	TN	4/2/2015	Paper Data	Medical/Healthcare	Yes - Published #	862

Cigna-HealthSpring TN Health Plan 862 04/02/2015 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Cigna-Health Spring
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
ITRC20150413-03	PIH Health Hospital - Whittier	CA	4/2/2015	Paper Data	Medical/Healthcare	Yes - Published #	826

PIH Health Hospital - Whittier CA Healthcare Provider 826 04/02/2015 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: PIH Health Hospital - Whittier
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
ITRC20150413-02	SUPERVALU Group Health Plan	IL	4/3/2015	Electronic	Medical/Healthcare	Yes - Published #	782

Attribution 1 Publication: hhs.gov Author:
Article Title: SUPERVALU Group 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
ITRC20150413-01	Covenant Ministries of Benevolance	IL	4/3/2015	Electronic	Medical/Healthcare	Yes - Published #	782

Health Plan sponsored by Covenant Ministries of Benevolance IL Health Plan 782 04/03/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Health Plan sponsored by Covenant Ministries of Benevolance
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
ITRC20150409-01	White Lodging Services Corp.	IN	4/9/2015	Electronic	Business	Yes - Unknown #	Unknown

A data breach that affected a downtown Louisville hotel is being investigated by law enforcement officials, according to an announcement from White Lodging Services Corp. According to the company, the suspected data breach affected point-of-sales systems at food and beverage outlets within the hotels. The Louisville Marriott Downtown at 280 W. Jefferson St. was among 10 hotels affected. White Lodging contracts with various hotel chains to manage the day-to-day operations of the hotels.

Attribution 1 Publication: Austin Business Journal Author: Michael Theis
Article Title: Downtown Louisville hotel hit by data breach; credit card info at risk
Article URL: http://www.bizjournals.com/louisville/blog/morning_call/2015/04/downtown-louisville-hotel-hit-by-data-breach.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150408-06	District of Columbia Public Schools	DC	2/4/2015	Electronic	Educational	Yes - Unknown #	Unknown

D.C. Public Schools says they recently learned of a data breach that left sensitive student information and passwords exposed. The breach allowed public access to an internal website that contained information pertaining to special education students. The site was launched in 2010 and stores training materials and database login information.

Attribution 1 Publication: Author:
Article Title: DC Public Schools say data breach left student information, passwords exposed
Article URL: http://www.myfoxdc.com/story/28021428/dc-public-schools-say-data-break-left-student-information-passwords-expos

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150408-05	University of California Riverside	CA	4/7/2015	Electronic	Educational	Yes - Published #	8,000

UC Riverside officials are notifying 8,000 graduate students and graduate applicants that their personal identity information is at risk. A desktop computer stolen during a break-in at the campus' graduate division offices March 13 contained the Social Security numbers of the students and potential students. Officials said they had no evidence that the information has been used for identity theft and they have no leads on who stole the computer.

Attribution 1 Publication: The Press Enterprise Author: Mark Muckenfuss
Article Title: UC RIVERSIDE: Computer stolen; data breach affects 8,000
Article URL: http://www.pe.com/articles/information-764066-computer-lovekin.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150408-04	Retail Capital, LLC	MI	4/2/2015	Electronic	Banking/Credit/Financial	Yes - Published #	741

We write to you with important information about a potential ·compromise of certain personal information that occurred on March 17, 2015. The incident involved unauthorized access by an unidentified third party to the electronic mailbox of one of our sales managers. The intruder was able illicitly to acquire the manager's password, thereby gaining access to the manager's electronic mailbox. Upon gaining access, the intruder locked our employee out of the mailbox. We identified the intrusion and re-established the security of the mailbox within approximately 40 minutes.

Attribution 1 Publication: NH AG's office / Scmagazine.com Author:
Article Title: Retail Capital, LLC
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/retail-capital-20150401.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150408-03	Momentive Performance Materials Savings Plan	OH	4/3/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On January 28, 2015, information about participants in the Momentive Performance Materials Savings Plan was inadvertently included in a file that was sent by Fidelity to another Fidelity client firm. The file was only accessible by one employee at the client firm through a password-protected Web application. When the employee realized that the data did not belong to her company's plan, she notified Fidelity. The file included for each participant: name, Social Security number, plan number, status, annual salary amount, effective date and last update.

Attribution 1 Publication: NH AG's office Author:
Article Title: Momentive Performance Materials Savings Plan (Fidelity Investments)
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/momentive-performance-20150401.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150408-02	Franklin & Marshall College	PA	4/2/2015	Electronic	Educational	Yes - Published #	356

On March 19,2015, Franklin & Marshall was notified that Excel files containing some students' personal information had been posted to a public portion of Franklin & Marshall's network. We immediately began an investigation and removed the spreadsheets from public view. Our investigation determined that a Franklin & Marshall employee had accidently posted the files to the college's public network. The two files were publicly available from March 27, 2013, and June 13, 2013, respectively, and were both removed from public access on March 19, 2015. The files contained students' full names and Social Security numbers

Attribution 1 Publication: NH AG's office Author:
Article Title: Franklin & Marshall College
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/franklin-marshall-college-20150402.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150408-01	City of Philadelphia - Fire Department EMS Unit	PA	4/2/2015	Electronic	Government/Military	Yes - Published #	81,463

The Philadelphia Fire Department (the “Fire Department”) learned of a data breach that affects individuals who used its ambulance services between February 1, 2012 and September 4, 2012. The data breach occurred between June 1, 2012 and October 2, 2012, during which time an employee of Advanced Data Processing, Inc., a subsidiary of Intermedix Holdings Inc., disclosed patient account information to a theft ring involved in a scheme to file fraudulent tax returns with the Internal Revenue Service. Advanced Data Processing, Inc. (conducting business under the name “Intermedix”) handles billing services for ambulance agencies throughout the nation, including Emergency Medical Services (“EMS”), the unit of the Fire Department that provides ambulance services in Philadelphia.

Attribution 1 Publication: hhs.gov / Philadelphia Fire Department Author:
Article Title: City of Philadelphia - Fire Department EMS Unit
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
ITRC20150407-06	Office of Elizabeth Kerner, M.D.	TX	4/3/2015	Electronic	Medical/Healthcare	Yes - Published #	873

Elizabeth Kerner, M.D. TX Healthcare Provider 873 04/03/2015 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Elizabeth Kerner, M.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
ITRC20150407-05	Department of Business Oversight	CA	4/7/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

The California Public Records Act (PRA) requires the Department of Business Oversight (DBO) to provide the public copies of the non-confidential portions of our electronic licensing records upon request. To process these requests, DBO utilizes the records contained in the Financial Industry Regulatory Authority’s (FINRA) Central Registration Depository (CRD). Fields clearly designated as containing personal identifying information within the FINRA CRD are then redacted by DBO prior to its release. However, despite our efforts, DBO recently learned that, pursuant to one or more PRA requests, the personal identifying information of a number of registered investment advisers and broker-dealers was inadvertently disclosed to persons not authorized to receive such information.

Attribution 1 Publication: CA AG's office Author:
Article Title: Department of Business Oversight
Article URL: https://oag.ca.gov/system/files/SDD%20Breach%20Notification%20Letter%20for%20DOJ_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150407-04	Law Enforcement - American Express	AL	4/7/2015	Electronic	Business	Yes - Unknown #	Unknown

We are strongly committed to the security of our Cardmembers’ information and strive to let you know about security concerns as soon as possible. We were recently made aware that your American Express Card information was recovered during an investigation by law enforcement and/or American Express. At this time, we believe the recovered data included your American Express Card account number, your name and other Card information such as the expiration date and your Social Security number. Importantly our systems have not detected any unauthorized activity on your Card account related to this incident.

Attribution 1 Publication: CA AG's office Author:
Article Title: Law Enforcement - American Express
Article URL: https://oag.ca.gov/system/files/CA%20AG%20Online%20Submission_%20C2015020316_Customer%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150407-03	Auburn University	AL	4/2/2015	Electronic	Educational	Yes - Published #	364,012

On March 2, 2015, Auburn University became aware of the fact that personal information relating to certain current, former, and prospective students was inadvertently accessible on the internet since September 2014. Auburn University corrected this internal issue the day it was discovered and retained independent forensics experts to identify the full extent of data implicated by this situation.

Attribution 1 Publication: CA AG's office / Scmagazine.com Author:
Article Title: Auburn University
Article URL: https://oag.ca.gov/system/files/Auburn%20-%20notice%20sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150407-02	SRI, Inc.	VA	4/2/2015	Electronic	Business	Yes - Published #	9,000

On March 13, 2015, SRI, Inc. ("SRI") learned of unauthorized access of our website software. We believe that unauthorized access may have been occurring since December 2014. An outside user may have been able to access files containing your persona l information. At this time, we have found no specific evidence that your particular information was actually viewed or downloaded. As soon as we were advised of the access, we began the process to remove personal information from our system in order to ensure personal information is no longer viewable.

Attribution 1 Publication: scmagazine.com / MD AG's office Author: Adam Greenberg
Article Title: ata at risk for 9,000 individuals following unauthorized access to SRI Inc. website
Article URL: http://www.scmagazine.com/data-at-risk-for-9000-individuals-following-unauthorized-access-to-sri-inc-website/article/

Attribution 2 Publication: CA AG's office / NH AG's office Author:
Article Title: SRI, Inc.
Article URL: https://oag.ca.gov/system/files/CA%20Template_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150407-01	Tulare County Health & Human Services	CA	4/6/2015	Electronic	Government/Military	Yes - Published #	845

We are sending this letter to you as part of Tulare County Health & Human Services Agency's (HHSA) commitment to patient privacy. We take patient privacy very seriously, and it is important to us that you are made fully aware of a potential privacy breach. We have learned that your information (specifically your email address associated with a patient at Visalia/Farmersville Healthcare Center) may have been compromised.

Attribution 1 Publication: CA AG's office Author:
Article Title: Tulare County Health & Human Services
Article URL: https://oag.ca.gov/system/files/Signed%20Notification%20Ltrs_Eng-Sp_4-1-15.pdf%20-%20Adobe%20Acrobat%20Pro_

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150403-02	7-11, Inc. Comprehensive Welfare Benefits Plan No. 525	TX	4/3/2015	Electronic	Medical/Healthcare	Yes - Published #	1,688

7-Eleven, Inc. Comprehensive Welfare Benefits Plan No. 525 TX Health Plan 1688 03/25/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: 7-11, Inc. Comprehensive Welfare Benefits Plan No. 525
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
ITRC20150401-03	**Bradley University**	IL	4/1/2015	Electronic	Educational	Yes - Published #	**4,700**

Bradley University is reporting a data breach that exposed personal information of employees and their families. In a news release, the private Illinois school says an internal investigation conducted over the last several days discovered malware on two University computers containing personal information. Bradley says malware may have captured personal information, including social security numbers. The University has received reports from employees indicating fraudulent tax return filings.

Attribution 1 Publication: KWQC.com Author:
Article Title: Security breach impacts employees at Bradley University
Article URL: http://kwqc.com/2015/03/31/security-breach-impacts-employees-at-bradley-university/

Attribution 2 Publication: cinewsnow.com / datalossdb.org Author: WEEK Reporter
Article Title: FBI, IRS and Bradley University investigating data breach leaving thousands vulnerable
Article URL: http://www.cinewsnow.com/news/local/FBI-IRS-and-Bradley-University-investigating-data-breach-leaving-thousands-v

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150401-02	**McDermott Will & Emery**	IL	4/1/2015	Electronic	Medical/Healthcare	Yes - Published #	**880**

McDermott Will & Emery LLP is the plan sponsor for the McDermott medical plan IL Health Plan 880 03/24/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: McDermott Will & Emery
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
ITRC20150401-01	**Freelancers Insurance Company**	NY	4/1/2015	Electronic	Medical/Healthcare	Yes - Published #	**43,068**

Freelancers Insurance Company NY Health Plan 43068 03/24/2015 Hacking/IT Incident Network Server

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-28	**Department of Labor**	VT	3/20/2015	Electronic	Government/Military	Yes - Published #	**80**

The Vermont Department of Labor has determined a now-former employee improperly obtained "personally identifiable information" including names and Social Security numbers from its unemployment insurance program database. A criminal investigation into possible identity theft is underway, officials said. At least 80 people are affected by the breach. Also at least seven businesses have been compromised, officials said.

Attribution 1 Publication: Burlington Free Press / VT AG's office Author:
Article Title: Records ID state worker accused in data breach
Article URL: http://www.burlingtonfreepress.com/story/news/local/vermont/2015/03/20/labor-department-says-employee-stole-ssns/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-27	**BetterBee.com**	NY	3/16/2015	Electronic	Business	Yes - Published #	**332**

WebSitePipeline (WSP) reports to us that at some point In the past, they had a hacker attack that successfully infiltrated one of their main computers and the hackers were able to obtain passwords for some of the companies using WSP. The hackers then were able to access the websites and upload malicious code. This code transmitted credit card data in duplicate. That code was uploaded on March 3, 2015.

Attribution 1 Publication: NH AG's office Author:
Article Title: BetterBee.com
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/betterbee-websitepipeline-20150316.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-26	Slack	CA	3/30/2015	Electronic	Business	Yes - Unknown #	Unknown

The group messaging provider Slack recently announced that a database storing user profile information, including user names, email addresses and hashed passwords, was breached during a four-day period in February 2015.

Attribution 1 Publication: esecurityplanet.com Author: Jeff Goldman
Article Title: Slack Hacked
Article URL: http://www.esecurityplanet.com/hackers/slack-hacked.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-25	Colonial Car Wash	NY	3/30/2015	Electronic	Business	Yes - Unknown #	Unknown

Rotterdam police Sunday warned the public about several debit and credit card breaches that occurred at the Colonial Car Wash starting in early March. Police were contacted by managers from M&T Bank, First Niagara and Price Chopper Federal Credit Union that there were several victims who had fraudulent activity on their accounts after using their cards at the 1530 Altamont Ave. business, police said.

Attribution 1 Publication: databreaches.net / timesunion.com Author:
Article Title: Colonial Car Wash
Article URL: http://www.timesunion.com/news/article/Colonial-Car-Wash-credit-breaches-investigated-6166614.php

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-24	ModSpace	PA	1/26/2015	Electronic	Business	Yes - Unknown #	Unknown

On September 19, 2014, we discovered that an employee who works in the company's Human Resources department emailed an unencrypted file containing personal information to an unauthorized third party. The personal information in the file included names, addresses, Social Security numbers, and insurance information.

Attribution 1 Publication: MD AG's office Author:
Article Title: ModSpace
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-251207.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-23	ValuTeachers, Inc.	GA	2/9/2015	Electronic	Business	Yes - Unknown #	Unknown

In particular, on February 02,2015, a ValuTeachers, Inc. employee sent an email that inadvertently included an attachment containing the names and social security numbers of insurance agents appointed with ValuTeachcrs. The email was sent to all of the insurance agents appointed with ValuTeachers at their ValuTeachers designated email address. The inadvertent disclosure was discovered immediately after the email was sent and ValuTeachers promptly disabled the ValuTcachers designated email accounts of the recipients of the email.

Attribution 1 Publication: MD AG's office Author:
Article Title: ValuTeachers, Inc.
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-251206.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-22	Hartford Surgical Associates, PA	MD	2/19/2015	Paper Data	Medical/Healthcare	Yes - Published #	350

On 10. 15.14, multiple patient billing statements for different patients were folded together. On 10.16. 14, the folded together bills were accidentally mailed in a single envelope to the patient name on the top statement. Thus, some of our patients received bills for up to three patients other than themselves. The bills may have included patient name, address, phone number, account number with our practice, and billing information

Attribution 1 Publication: MD AG's office Author:
Article Title: Hartford Surgical Associates, PA
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-251205.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-21	Kohl's	WI	2/5/2015	Electronic	Business	Yes - Unknown #	Unknown

The company recently was notified by its third-party call center of an incident involving the compromise of some personal information of certain Kohl's customers. A call center employee appears to have been capturing certain customer information for unauthorized purposes. The personal information obtained by the call center employee may have included certain customers' names, postal addresses, email addresses, telephone numbers, partial Social Security numbers, and payment card information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Kohl's
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-251180.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-20	BAE Systems	VA	2/19/2015	Electronic	Business	Yes - Unknown #	Unknown

In December 2014, during the course of litigation with a former employee, BAE Systems learned that the plaintiff received Company documents from another former employee (the "Second Employee"). These documents were removed from the Company by the Second Employee without authorization. A few of the documents- forms filed with the U.S. Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives -- contained the names, dates of birth, and social security numbers of a few current and former employees. Upon learning of this incident, the Company took action through the court and obtained the return of the documents from the plaintiff.

Attribution 1 Publication: MD AG's office Author:
Article Title: BAE Systems
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-251124.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-19	TD Bank	NJ	2/18/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We recently learned that one of our employees may have improperly obtained and used confidential customer information to fraudulently withdraw funds from customer accounts. The personal information may have included name, address, Social Security number and account number. This is an isolated incident and is being addressed through an internal investigation by our corporate security team and we have engaged local law enforcement.

Attribution 1 Publication: MD AG's office Author:
Article Title: TD Bank
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-251123.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-18	Cigna	CT	2/13/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On December 27, 2014, Cigna discovered that on December 27,2014 a customer was able to v iew medical claims information regarding another customer on the MyCigna mobile application. The medical claims information displayed in error included the Customer's first and last name, Cigna customer ID, account mm1ber, and claim number, service elate and type, physician name, status of the claim, along with billed and paid amounts.

Attribution 1 Publication: MD AG's office Author:
Article Title: Cigna
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-251122.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-17	OnDeck Capital, Inc.	NY	2/4/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

In accordance with the above-referenced provision of the Maryland law, I am contacting you on behalf of our client, OnDeck Capital, Inc., to inform you of a data security incident. In November and December 2014, OnDeck employees lost two password-protected laptopns in public locations. Despite immediate searches, the laptops were never recovered. After conducting an investigation of the incident, OnDeck determined that the laptops contained personal information of three (3) Maryland residents, including names, Social Security numbers and bank account numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: OnDeck Capital, Inc.
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-250966.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-16	**Nationstar Mortgage / Corelogic Solutions Express**	TX	3/8/2015	Electronic	Banking/Credit/Financial	Yes - Published #	**34**

We are writing to inform you of an incident involving personal information security breach. On or about October 31, 2014, an incident occurred where Fedex lost a total of 34 loan modification documents in transit between our vendor CoreLogic Solutions Express in Sunrise, FL and Nationstar Mortgage in Lewisville, TX. The information comprised included: the loan number, borrower name, property address, UPB, mortgage recording information, and borrower signature.

Attribution 1 Publication: MD AG's office Author:
Article Title: Nationstar Mortgage / Corelogic Solutions Express
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-250963%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-15	**Frederick County Public Schools**	MD	2/12/2015	Electronic	Educational	Yes - Published #	**7,933**

I represent the Frederick County Public Schools (FCPS), located at 191 South East Street, Frederick, Maryland 21701. I am sending this letter pursuant to Md. Code Ann. Comm. Law § 14-3504 because FCPS was recently notified of an incident in which the W-2 information of approximately 7,933 Maryland residents may have been accessed without authorization. The W-2 information resided on an FCPS employee portal on the FCPS website, and included names, addresses, Social Security numbers, and wage and tax information

Attribution 1 Publication: MD AG's office Author:
Article Title: Frederick County Public Schools
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-250962%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-14	**gategroup**	VA	2/20/2015	Electronic	Business	Yes - Unknown #	**Unknown**

The security of its employees' personal information is very important to gategroup. The investigation into this matter is ongoing, but it has been determined that certain current and former employees' W-2 forms were subject to unauthorized access. These forms contain the name, address, Social Security number, and tax information of two (2) Maryland residents. It is believed the unauthorized access was disabled on the same day that it was discovered, and gategroup and its forensic experts are taking the necessary steps to confirm this fact.

Attribution 1 Publication: MD AG's office Author:
Article Title: gategroup
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-250958.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-13	**Gallagher Bassett**	CA	2/24/2015	Electronic	Business	Yes - Unknown #	**Unknown**

On February 10, 2015, Gallagher Bassett learned that a member of our claims adjustment team was a victim of theft during the process of home relocation on February 8, 2015, which included the theft of her work desktop computer and a limited batch of paper files. Gallagher Bassett immediately started its investigation to determine what information may be at risk as a result of the theft. We discovered that the hard drive of the desktop computer and paper files may have contained some personal information, including name, address, social security number, and/or some claim information, of the affected residents that was reviewed by the claims adjuster while processing the affected residents' claims.

Attribution 1 Publication: MD AG's office Author:
Article Title: Gallagher Bassett
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-250805.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-12	Columbia Management	MA	1/20/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

An error occurred during an upgrade to the Columbia Management website. An incorrect setting within the software allowed a registered user to log in and view a report containing information of other plan participants. The error was discovered during testing and promptly corrected. Unfortunately, these clients' personal information may have been viewed by another Columbia Management registered user during this period of time.

Attribution 1 Publication: MD AG's office Author:
Article Title: Columbia Management
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-251210.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-11	Citizens Financial Group	RI	1/16/2015	Electronic	Banking/Credit/Financial	Yes - Published #	1,813

On December 4, 2014, it was reported that a number of Citizens customers from Rhode Island and Connecticut had been contacted by someone representing themselves as an agent of a company where Citizens annuities were held (5 various companies). The stated reason for the call was that the customer was holding a matured product and the caller would like to set up an appointment to discuss options.

Attribution 1 Publication: MD AG's office Author:
Article Title: Citizens Financial Group
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-250975%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-10	Westmont College	CA	1/26/2015	Electronic	Educational	Yes - Unknown #	Unknown

We represent Westmont College (“Westmont”) with respect to a recent security incident involving the potential exposure of certain personally identifiable information described in more detail below. On December 12, 2014, a college laptop was stolen from a professor’s car that was briefly parked at a gas station. It appears that a number of applications for certain summer programs may have been on the laptop and may have contained the name, Social Security number, and other limited personal information of a limited number of students. Number of Maryland residents affected.

Attribution 1 Publication: MD AG's office / databreaches.net Author:
Article Title: Westmont College
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-250973.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-09	Chubb & Son	NJ	1/30/2015	Electronic	Business	Yes - Unknown #	Unknown

I am writing to you on behalf of my client, Chubb & Son, a division of Federal Insurance Company ("Chubb"), to advise you that on December 3, 2014, Chubb detected a suspicious file on an employee's computer. A comprehensive investigation conducted with the assistance of third-party computer forensics experts revealed the presence of unauthorized software on the computer which may have resulted in the acquisition of the personal information of a limited number of current and former employees.

Attribution 1 Publication: MD AG's office Author:
Article Title: Chubb & Son
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-250969.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-08	Charlotte Russe / Innotrac	CA	1/7/2015	Electronic	Business	Yes - Unknown #	Unknown

Innotrac provides global e-commerce fulfillment for leading brands, including Charlotte Russe. It performs stringent background checks on all of its employees, and monitors their communications. Nonetheless, Innotrac recently discovered that in December 2014 a seasonal employee at a call center it operates on behalf of Charlotte Russe appeared to have impermissibly accessed and used customer information she obtained while handling Charlotte Russe sales orders.

Attribution 1 Publication: MD AG's office Author:
Article Title: Charlotte Russe / Innotrac
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248527%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-07	Aetna	CT	1/8/2015	Electronic	Medical/Healthcare	Yes - Published #	133

On December 2, 2014, Aetna's Investigative Services unit received notification from the IRS that a former Aetna employee had been arrested in Florida. The arrest took place in April 2014. The individual stopped working for Aetna in August 2013. The former employee's personal cell phone was confiscated and pictures of screen shots from Aetna computer screens were found on it. The IRS has the cell phone and is conducting a criminal investigation of possible identity theft.

Attribution 1 Publication: MD AG's office Author:
Article Title: Aetna
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248526%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-06	Direct Marketing Association (DMA)	NY	1/8/2015	Electronic	Business	Yes - Unknown #	Unknown

This letter is to notify you that the Direct Marketing Association ("DMA") has experienced a data security incident involving our online bookstore. Other sections of the DMA website were not affected by this incident. Because our records show that you made one or more credit or debit card purchases through our bookstore during the relevant time period, we are writing to inform you that there may have been unauthorized access to credit and debit card data for the card(s) used in your transaction(s).

Attribution 1 Publication: MD AG's office Author:
Article Title: Direct Marketing Association (DMA)
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248525.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-05	Coulter Ventures, LLC (Rogue Fitness)	OH	1/6/2015	Electronic	Business	Yes - Published #	226

Pursuant to your state law, we are writing to inform you of a recent data incident involving Coulter Ventures, LLC d/b/a Rogue Fitness, headquartered in Columbus, Ohio. At this time it is believed that one resident of your state was potentially affected. We recently discovered a limited number of email attachments sent by customers to our company were publicly accessible on the Internet. From what we have determined, some of these attachments contained financial account information or social security information along with names, email addresses, or possibly mailing addresses.

Attribution 1 Publication: MD AG's office Author:
Article Title: Coulter Ventures, LLC (Rogue Fitness)
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248459.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-04	Nite Ize, Inc.	CO	3/27/2015	Electronic	Business	Yes - Unknown #	Unknown

Our consumer-facing website, www.niteize.com, is hosted and managed by a third-party website services provider. We recently learned from our service provider that our online store was subject to an attack in early March, and as a result, certain customer information may have been accessed by unauthorized parties. We immediately worked with our website provider to block the attack, repair the system, and investigate the incident and damage it caused. At this time, we cannot confirm that your data was stolen but are sending you this letter in an abundance of caution.

Attribution 1 Publication: CA AG's office / databreaches.net Author:
Article Title: Nite Ize, Inc.
Article URL: https://oag.ca.gov/system/files/Nite%20Ize%20Notification%20Letter%20Databse%20Only%20%28US%20incl%20PR%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-03	Kane Hall Barry Neurology	TX	3/19/2015	Electronic	Medical/Healthcare	Yes - Published #	600

Kane Hall Barry Neurology TX Healthcare Provider 600 03/19/2015 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Kane Hall Barry Neurology
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
ITRC20150330-02	GA Department of Community Health (#2)	GA	3/2/2015	Electronic	Government/Military	Yes - Published #	355,127

Georgia Department of Community Health GA Health Plan 355127 03/02/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Department of Community Health (#2)
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150330-01	GA Department of Community Health	GA	3/2/2015	Electronic	Government/Military	Yes - Published #	557,779

Georgia Department of Community Health GA Health Plan 557779 03/02/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Department of Community 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
ITRC20150329-04	Career Education Corporation	IL	3/19/2015	Electronic	Educational	Yes - Published #	151,626

Career Education Corporation IL Health Plan 2743 03/19/2015 Hacking/IT Incident Network

Attribution 1 Publication: hhs.gov Author:
Article Title: Career Education Corporation
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
ITRC20150329-03	Mount Sinai Medical Center	FL	3/20/2015	Paper Data	Medical/Healthcare	Yes - Published #	1,406

Mount Sinai Medical Center FL Healthcare Provider 1406 03/20/2015 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Mount Sinai 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
ITRC20150329-02	Life Care Center of Attleboro	MA	3/20/2015	Paper Data	Medical/Healthcare	Yes - Published #	2,473

Life Care Center of Attleboro in Massachusetts posted two separate announcements on its website about a potential PHI data breach after the company that stores its patient records could not find certain documents. Iron Mountain archives patient records for Life Care, and informed the company that after it had performed a limited audit on November 18, 2014, it could not find some boxes containing patient information. Specifically, if individuals were patients at the facility between 1992 and 2004, in 2006, or in 2011, their data was potentially compromised. Employees who worked at Life Care between 1992 and 1999 could also be affected.patientrecordsimage

Attribution 1 Publication: hhs.gov / healthitsecurity.com Author:
Article Title: PHI Data Breach Announced Following Audit
Article URL: http://healthitsecurity.com/2015/04/01/phi-data-breach-announced-following-audit/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150329-01	AT&T Group Health Plan	TX	3/23/2015	Electronic	Medical/Healthcare	Yes - Published #	50,000

AT&T Group Health Plan TX Health Plan 50,000 3/23/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: AT&T Group 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
ITRC20150323-04	Twitch	CA	3/23/2015	Electronic	Business	Yes - Unknown #	Unknown

We are writing to let you know that there may have been unauthorized access to some Twitch user account information. For your protection, we have expired passwords and stream keys and have disconnected accounts from Twitter and YouTube. As a result, you will be prompted to create a new password the next time you attempt to log into your Twitch account.

Attribution 1 Publication: databreaches.net / Twitch website Author:
Article Title: Twitch Security Breach Reported, Password Change Required
Article URL: http://www.databreaches.net/twitch-security-breach-reported-password-change-required/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150323-03	Hilton Hhonors Program	TX	3/23/2015	Electronic	Business	Yes - Unknown #	Unknown

The vulnerability allowed attackers to access any HHonors account simply by knowing or guessing the account number.
Bancsec security researchers Brandon Potter and JB Snyder recently discovered a security flaw in Hilton's website that allowed an attacker to access any Hilton HHonors account simply by knowing or guessing the account number, according to investigative reporter Brian Krebs.

Attribution 1 Publication: esecurityplanet.com Author: Jeff Goldman
Article Title: Massive Security Flaw Found in Hilton HHonors Website
Article URL: http://www.esecurityplanet.com/network-security/massive-security-flaw-found-in-hilton-hhonors-website.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150323-02	Aventura Hospital and Medical Center	FL	2/27/2015	Electronic	Medical/Healthcare	Yes - Published #	686

Aventura Hospital and Medical Center FL Healthcare Provider 686 02/27/2015 Unauthorized Access/Disclosure Desktop Computer, Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: Aventura Hospital and 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
ITRC20150323-01	Virginia Department of Medical Assistance (VA-	VA	3/12/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

Virginia Department of Medical Assistance Services (VA-DMAS) VA Health Plan 697,586 03/12/2015 Hacking/IT Incident Network Server No PART OF THE OVERALL TOTAL FOR ANTHEM

Attribution 1 Publication: hhs.gov Author:
Article Title: Virginia Department of Medical Assistance (VA-DMAS)
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Attribution 2 Publication: healthcareinfosecurity.com Author:
Article Title: Breach Tally Shows More Hacker Attacks
Article URL: http://www.healthcareinfosecurity.com/breach-tally-shows-more-hacker-attacks-a-8183/op-1

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150320-06	Tom Bradley International Terminal	CA	3/19/2015	Electronic	Business	Yes - Unknown #	Unknown

Authorities say they're investigating reports that debit and credit card information has been taken from a terminal at Los Angeles International Airport.
Airport officials said in a statement that 19 victims have been identified so far, and all of them work at LAX.

Attribution 1 Publication: losangeles.cbslocal.com Author:
Article Title: 19 Airport Employees ID'd As Victims Of Possible Credit Card Breach At LAX Terminal
Article URL: http://losangeles.cbslocal.com/2015/03/19/19-airport-employees-idd-as-victims-of-possible-credit-card-breach-at-lax-te

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150320-05	Equifax	GA	3/19/2015	Electronic	Business	Yes - Published #	300

A CBS 13 investigation has launched a state level probe into one of the three major credit reporting bureaus. Your personal and private information may be caught in the middle as we discovered what appears to be a data breach involving an agency responsible for keeping track of all your financial information. By now we're all familiar with hackers breaking in to systems and stealing sensitive information from retailers - like they did with Target, Home Depot, Shaws and Michaels, but this incident involving Equifax is very different; it looks like they just gave the information away. A woman right here in Maine got hundreds of credit reports in the mail, all addressed to her, but belonging to other people all over the country.

Attribution 1 Publication: NH AG's office Author:
Article Title: Equifax
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/equifax-20150402.pdf

Attribution 2 Publication: wgme.com / databreaches.net Author:
Article Title: 13 Investigates: Equifax mistakenly sends hundreds of credit reports to Biddeford woman
Article URL: http://wgme.com/news/features/top-stories/stories/13-investigates-hundreds-credit-reports-mistakenly-sent-biddeford-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150320-04	Florida Hospital	FL	3/20/2015	Paper Data	Medical/Healthcare	Yes - Published #	8,700

On May 2, 2014, we were notified that Florida Hospital facesheets (a summary cover sheet to a patient's medical record) were discovered in the course of an investigation being conducted by law enforcement. While working with law enforcement, we determined two Florida Hospital employees printed patient facesheets outside of their normal job duties, which may have contained patents' names, addresses, Social Security numbers, phone numbers, emergency contact information, health insurance information and certain health information such as physician names and diagnoses.

Attribution 1 Publication: databreaches.net / hhs.net Author:
Article Title: Florida Hospital discloses another insider breach
Article URL: http://www.databreaches.net/florida-hospital-discloses-another-insider-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150320-03	Capital One	VA	3/16/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We were recently notified by law enforcement that a former employee, while still employed at Capital One® , passed on your information to an unauthorized third party. This was followed by attempted charges on your account with us. As you know, on <AdhocVar1>, we shut down that card and sent you a new card with a new account number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150320-02	EyeCare of Bartlesville	OK	3/13/2015	Electronic	Medical/Healthcare	Yes - Published #	4,000

On February 20, 2015 the computer housing our patient database was compromised by an outside malware virus. To the best of our knowledge and the knowledge of our computer expert handling the situation, we do not believe any information was taken from the computer. The computer hard drive has been locked and is no longer accessible. Unfortunately, we cannot with 100% certainty guarantee that no information was taken. We felt it our duty to notify our patients of the potential security breach.

Attribution 1 Publication: hhs.gov / databreaches.net Author:
Article Title: EyeCare of Bartlesville
Article URL: http://www.databreaches.net/ok-eyecare-of-bartlesville-notifies-patients-after-hard-drive-locked-by-malware/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150320-01	Advance Rehabilitation & Consulting LTD	GA	3/2/2015	Electronic	Medical/Healthcare	Yes - Published #	570

Advance Rehabilitation & Consulting LTD GA Healthcare Provider 570 03/02/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Advanced Rehabilitation & Consulting 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
ITRC20150319-02	Shell Vacations Club-West	FL	1/6/2015	Paper Data	Business	Yes - Unknown #	Unknown

On behalf of SVC-West, LLC ("SVC"), a part of Shell Vacations Club, I am writing to inform you about an incident where certain personal information of some of our owners, including you, may have been taken as a result of a break-in at a California office. While we take reasonable steps to protect our records, in January 2015 an unknown individual(s) forcibly and illegally entered an office and stole items from a locked cabinet that included a binder containing records of transactions with SVC during 2005 to 2008. These records included personal information such as some owners' name, address, driver's license number, Social Security number and/or financial information (i.e., payment card numbers and/or financial account numbers).

Attribution 1 Publication: CA AG's office Author:
Article Title: Shell Vacations Club-West
Article URL: https://oag.ca.gov/system/files/SVC_West_NON-MA%20US%20CONSUMER%20LTR_SAMPLE_031715_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150319-01	Apple American Group (Applebee's)	OH	3/3/2015	Electronic	Business	Yes - Published #	3,058

We are contacting you regarding a data security incident that occurred on March 3, 2015, involving your W-2 information. On that date, an outside consultant (that is, someone who is not an employee of Apple American Group, but rather a third party vendor hired to help us improve our payroll systems) lost a portable USB flash drive. We have learned this flash drive contained your name, address, Social Security number, wage and tax information. (3,058 = Indiana)

Attribution 1 Publication: CA AG's office / MD AG's office Author:
Article Title: Apple American Group
Article URL: https://oag.ca.gov/system/files/Non-Massachusetts%20consumer%20notification%20letter%20FINAL%20AAG_0.PDF?

Attribution 2 Publication: indystar.com Author:
Article Title: Indiana's top 10 data breaches so far this year
Article URL: http://www.indystar.com/story/money/2015/07/18/indianas-top-10-data-breaches-so-far-year/30360027/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150318-11	Texas A&M	TX	3/15/2015	Electronic	Educational	Yes - Published #	4,697

The social security numbers for 4,697 faculty and graduate assistants who taught during the Fall 2014 semester at Texas A&M University were viewable from a department website. The social security numbers were inadvertently displayed along with the individual's first and last name in the Fall 2014 Semester Teaching Analysis Report (STAR). Upon discovering the situation, the University immediately removed access to the website and sent letters to those that might have been impacted by this data breach.

Attribution 1 Publication: databreaches.net Author:
Article Title: Texas A&M Data Breach of Nearly 4,700 Faculty & Graduate Assistants
Article URL: http://www.databreaches.net/texas-am-data-breach-of-nearly-4700-faculty-graduate-assistants/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150318-10	Sacred Heart Health System (Ascension Health)	FL	3/16/2015	Electronic	Medical/Healthcare	Yes - Published #	14,177

The privacy and security of patient information is of utmost importance to Sacred Heart Health System, Inc. and we have implemented significant security measures to protect such information. Regrettably, despite Sacred Heart's efforts to safeguard patient information, a hacking attack has affected Sacred Heart patients. On February 2, 2015, we were notified by one of our third-party billing vendors that one of its employee's e-mail user name and password had been compromised as a result of an e-mail hacking attack. The hacking attack was detected by our billing vendor on December 3, 2014 and the employee's user name and password were shut down the same day.

Attribution 1 Publication: databreaches.net / SHHS website Author:
Article Title: Sacred Heart Health System billing information hacked
Article URL: http://www.databreaches.net/fl-sacred-heart-health-system-billing-information-hacked/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150318-09	E.K. and Company (Mark Riley, Inc.)	CA	3/17/2015	Electronic	Business	Yes - Unknown #	Unknown

Mark Riley, Inc. dba E. K. and Company ("E. K. and Company") is an accounting and payroll processing company. On January 19, 2015, E. K. and Company's office was broken into and a hard drive was stolen. This hard drive may have contained data files that include your name, Social Security number, address, telephone number, and financial account information. While this information could not be accessed without the tax preparation software, which was not on the hard drive, we wanted to make you aware of this event out of an abundance of caution.

Attribution 1 Publication: databreaches.net Author:
Article Title: E. K. and Company notifies clients of stolen hard drive with financial information
Article URL: http://www.databreaches.net/e-k-and-company-notifies-clients-of-stolen-hard-drive-with-financial-information/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150318-08	EMC	MA	3/18/2015	Paper Data	Business	Yes - Unknown #	Unknown

I received an interesting letter in the mail yesterday from EMC Corporation. It seems that at some point in the last two months of 2014 they managed to lose control of my basic personal information, including my date of birth and Social Security number -- giving the ability to whoever acquired the data to take a pretty good shot at identity theft.

Attribution 1 Publication: databreaches.net / ZDNet / EMC letter Author:
Article Title: EMC
Article URL: http://www.zdnet.com/article/emc-data-security-fails-the-old-fashion-way/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150318-07	Alta Ski Area	UT	3/3/2015	Electronic	Business	Yes - Unknown #	Unknown

We are contacting you because we have reason to believe that your credit card information may have been accessed by unauthorized person(s) from a foreign Internet address. Alta does not store credit card numbers of its customers. However, on February 16, 2015, unauthorized person(s) executed a sophisticated attack on the checkout portion of Alta's estore which allowed them to collect credit card information from Alta customers purchasing lifts tickets online

Attribution 1 Publication: VT AG's office Author:
Article Title: Alta Ski Area
Article URL: http://www.ago.vermont.gov/assets/files/Consumer/Security_Breach/Alta%20Ski%20Lifts%20SBN%20to%20Consumer

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150318-06	Amedisys	CA	3/15/2015	Electronic	Medical/Healthcare	Yes - Published #	6,909

Home health and hospice company Amedisys recently discovered that it had 142 missing encrypted devices during a risk management process. The organization said in a statement that it sent out notification letters to 6,909 individuals whose information was potentially compromised.

Attribution 1 Publication: healthitsecurity.net / MD AG's office Author: Elizabeth Snell
Article Title: Missing Encrypted Devices Leads to 7K Notification Letters
Article URL: http://healthitsecurity.com/2015/03/16/missing-encrypted-devices-leads-to-7k-notification-letters/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150318-05	Kaiser Foundation Health Plan of the Mid-Atlantic	MD	1/29/2015	Paper Data	Medical/Healthcare	Yes - Published #	630

Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc. MD Health Plan 630 01/29/2015 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Kaiser Foundation Health Plan of the Mid-Atlantic States
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
ITRC20150318-04	County of Haywood	NC	2/9/2015	Paper Data	Government/Military	Yes - Published #	955

Haywood County NC NC Healthcare Provider 955 02/09/2015 Loss Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: County of Haywood
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
ITRC20150318-03	Children's National Health System	DC	2/24/2015	Electronic	Medical/Healthcare	Yes - Published #	18,000

On December 26, 2014, Children's National learned that certain employee email accounts had been potentially exposed in a way that may have allowed hackers to access information contained in those email accounts. This was a result of employees having received "phishing" emails and responding believing they were legitimate. This may have created an opportunity for unauthorized access to these individual email accounts from July 26, 2014 to December 26, 2014.

Attribution 1 Publication: hhs.gov / databreaches.net / healthitsec Author:
Article Title: Children's National Health System notified 18,000 patients after employees fell for phishing scheme
Article URL: http://www.databreaches.net/childrens-national-health-system-notified-18000-patients-after-employees-fell-for-phishin

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150318-02	Advantage Dental (Advantage Consolidated LLC)	OR	3/17/2015	Electronic	Medical/Healthcare	Yes - Published #	151,626

A company with more than 30 dental clinics serving low-income people in Oregon says it's been hacked, and the intruders got Social Security numbers and other personal information, but not treatment or financial data. Advantage Dental, of Redmond, is notifying patients and paying for an identity-theft monitoring service, The Bulletin newspaper of Bend reported Tuesday (http://bit.ly/1GZ6LsW). An intruder breached its internal membership database in late February and accessed information on more than 151,000 patients, said Jeff Dover, Advantage's compliance manager.

Attribution 1 Publication: dailyastorian.com Author:
Article Title: Dental company for low-income Oregonians reports data breach
Article URL: http://www.dailyastorian.com/dental-company-for-low-income-oregonians-reports-data-breach-da-ap-webfeeds-news-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150318-01	Premera Blue Cross	WA	3/17/2015	Electronic	Medical/Healthcare	Yes - Published #	11,000,000

Premera Blue Cross, a major provider of health care services, disclosed today that an intrusion into its network may have resulted in the breach of financial and medical records of 11 million customers. Although Premera isn't saying so just yet, there are indicators that this intrusion is once again the work of state-sponsored espionage groups based in China. In a statement posted on a Web site set up to share information about the breach — premeraupdate.com — the company said that it learned about the attack on January 29, 2015. Premera said its investigation revealed that the initial attack occurred on May 5, 2014. "This incident affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and our affiliate brands Vivacity and Connexion Insurance Solutions, Inc," the company said. Their statement continues:

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Premera Blue Cross Breach Exposes Financial, Medical Records
Article URL: http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150313-02	Providence ST. Joseph Medical Center / Providence	WA	2/18/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

We are writing to you about the disclosure of your medical billing information to one of our business partners. On February 18, 2015, Providence St. Joseph Medical Center discovered that a Providence staff member inadvertently sent your billing information to a company that handles billing for some of our physician medical groups that Providence contracts with in Southern California.

Attribution 1 Publication: CA AG's office Author:
Article Title: Providence Health & Services
Article URL: https://oag.ca.gov/system/files/Providence%20Adult%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150313-01	Aurora Health Care	WI	3/10/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Aurora Health Care recently discovered that we were the target of a criminal cyber attack that infected some workstations and servers with malware, or a type of computer virus. The malware had been installed on some of Aurora's workstations and servers and was designed to capture login information when users accessed certain websites, mostly financial in nature and some social media.

Attribution 1 Publication: VT AG's office Author:
Article Title: Aurora Health Care
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Aurora%20Health%20Care%20SBN%20to%20Consume

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150312-02	Clinical Reference Laboratory, Inc.	KS	3/3/2015	Paper Data	Medical/Healthcare	Yes - Published #	4,668

Clinical Reference Laboratory, Inc. KS Healthcare Provider 4,668 03/03/2015 LossPaper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Clinical Reference Laboratory, 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
ITRC20150312-01	Mosaic Medical	OR	3/5/2015	Electronic	Medical/Healthcare	Yes - Published #	2,207

Mosaic Medical OR Healthcare Provider 2,207 03/05/2015 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Mosaic Medical
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
ITRC20150311-02	TD Bank, N.A.	NJ	2/27/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

TD Bank, N.A. is notifying your office of a privacy event impacting 2 New Hampshire residents. Our investigation identified two of our customers who are residents of New Hampshire and may have been affected by this incident. We recently learned that one of our employees may have improperly obtained customer personal information and provided it to a third party not associated with TD Bank resulting in fraudulent activity on their accounts.

Attribution 1 Publication: NH AG's office Author:
Article Title: TD Bank, N.A.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/td-bank-20150220.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150311-01	Kraft Music LTD	WI	3/3/2015	Electronic	Business	Yes - Unknown #	Unknown

I write on behalf of my client, Kraft Music LTD ("Kraft," operator of the kraftmusic.com website: the "Website") to inform you of a security incident involving personal information provided to Kraft that affected approximately 5 New Hampshire residents.

Attribution 1 Publication: NH AG's office Author:
Article Title: Kraft Music LTD
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/kraft-music-20150303.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150310-02	Blue Cross Blue Shield - Michigan	MI	3/10/2015	Paper Data	Medical/Healthcare	Yes - Published #	5,514

Eleven people have been charged with identity theft and credit card fraud after a Blue Cross Blue Shield of Michigan employee allegedly printed and shared screen shots of more than 5,000 subscriber profiles.

Attribution 1 Publication: datalossdb.org / detroitnews.com Author:
Article Title: 11 charged in theft of Blue Cross subscriber info
Article URL: http://www.detroitnews.com/story/business/2015/03/10/charged-theft-blue-cross-subscriber-info/24711063/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150310-01	Bistro Burger (Epic Foods)	CA	3/10/2015	Electronic	Business	Yes - Unknown #	Unknown

California-based Bistro Burger is notifying customers of a payment card breach via notices on their web site and legal notices in the Los Angeles Times and the San Francisco Chronicle. Copies of the notices have been submitted to the California Attorney General's web site.

Attribution 1 Publication: databreaches.net / CA AG's office Author:
Article Title: Bistro Burger discloses payment card breach at Mission Street location
Article URL: http://www.databreaches.net/ca-bistro-burger-discloses-payment-card-breach-at-mission-street-location/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150309-08	Zoup / NEXTEP Systems	MI	3/9/2015	Electronic	Business	Yes - Unknown #	Unknown

NEXTEP Systems, a Troy, Mich.-based vendor of point-of-sale solutions for restaurants, corporate cafeterias, casinos, airports and other food service venues, was recently notified by law enforcement that some of its customer locations have been compromised in a potentially wide-ranging credit card breach, KrebsOnSecurity has learned. The acknowledgement came in response to reports by sources in the financial industry who spotted a pattern of fraud on credit cards all recently used at one of NEXTEP'S biggest customers: Zoup, a chain of some 75 soup eateries spread across the northern half of the United States and Canada.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Point-of-Sale Vendor NEXTEP Probes Breach
Article URL: http://krebsonsecurity.com/2015/03/point-of-sale-vendor-nextep-probes-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150309-07	Indiana State Medical Association	IN	3/6/2015	Electronic	Medical/Healthcare	Yes - Published #	38,351

On February 13, 2015, someone stole two archive backup hard drives containing the Indiana State Medical Association ("ISMA") group health and life insurance databases. The theft occurred while an ISMA employee was transporting the hard drives to an offsite storage location as part of our disaster recovery plan. This was a random criminal act. We discovered the theft the same day it occurred and reported the incident and all pertinent details to the Indianapolis Metropolitan Police Department (IMPD) to assist in their investigation. (38,351 per hhs.gov)

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Indiana State Medical Association discloses theft of backup drives with 39,090 members' health insurance information
Article URL: http://www.databreaches.net/indiana-state-medical-association-discloses-theft-of-backup-drives-with-39090-members-

Attribution 2 Publication: VT AG's office Author:
Article Title: Indiana State Medical Association
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/ISMA%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150309-06	A.C. Moore Arts & Crafts / Ascensus	PA	3/6/2015	Electronic	Business	Yes - Unknown #	Unknown

Ascensus, the recordkeeper for A.C. Moore Arts & Crafts, Inc. 401(k), is writing to notify you that on February 9, 2015, Ascensus inadvertently sent a report containing your name, address, birth date, and social security number to another Ascensus client. Upon discovering this, Ascensus immediately informed the client that the client received confidential data in error

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: A.C. Moore Arts & Crafts / Ascensus
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Ascensus%20Inc%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150309-05	Valley Community Healthcare	CA	3/9/2015	Electronic	Medical/Healthcare	Yes - Published #	1,223

On February 24, 2015 we discovered that a laptop computer attached to the Electrocardiogram (EKG) machine in the General Medicine department was missing. After searching the premises, the incident was reported to the North Hollywood Police Department (Report # 150224003504) that same day.

Attribution 1 Publication: CA AG's office / databreaches.net / hhs. Author:
Article Title: Valley Community Healthcare
Article URL: https://oag.ca.gov/system/files/Valley%20Community%20Breach%20Letter%2003-2015%20SRR%20Revised_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150309-04	Office of Sharon J. Jones, M.D.	CA	3/5/2015	Paper Data	Medical/Healthcare	Yes - Published #	1,342

On the evening of January 8, 2015, our office was broken into and our 2014 credit card transaction register and approximately 350 patient charts were stolen. Upon discovery the following morning, the San PabloPolice Department was immediately notified and a formal police report was filed. (1,342 per HHS.gov)

Attribution 1 Publication: phiprivacy.net Author:
Article Title: Physician notifies patients after burglars steal credit card transaction records and patient charts
Article URL: http://www.phiprivacy.net/ca-physician-notifies-patients-after-burglars-steal-credit-card-transaction-records-and-patie

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150309-03	St. Mary's (Health) Medical Center (Ascension Health)	IN	3/8/2015	Electronic	Medical/Healthcare	Yes - Published #	3,952

Around 4,400 people were recently sent letters by St. Mary's Medical Center informing them of a cyber attack on several hospital employees' email accounts that happened in January, according to Randy Capehart, St. Mary's spokesperson. Hackers gained access to health information contained in the emails, according to Capehart. Patient information was compromised, including name, date of birth, gender, date of service, insurance information, health information and Social Security numbers in some cases. Capehart said St. Mary's immediately shut down the email accounts. (3,952 per hhs.gov)

Attribution 1 Publication: phiprivacy.net / medical center website Author:
Article Title: St. Mary's Health: Patient information compromised in Email hack
Article URL: http://www.phiprivacy.net/in-st-marys-health-patient-information-compromised-in-email-hack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150309-02	San Francisco General Hospital	CA	3/6/2015	Electronic	Medical/Healthcare	Yes - Published #	2,500

A former UCSF doctor who worked at San Francisco General Hospital from 2005 to 2013 wrongfully removed copies of patient records from the medical center, public health officials said Friday. UCSF reported the security breach to the San Francisco Department of Public Health on Feb. 13. The incident is under investigation and authorities don't yet know how many patients were affected or when the files were taken. (2,500 per hhs.gov)

Attribution 1 Publication: phiprivacy.net / sfgate.come / hhs.gov Author: Erin Allday
Article Title: SF General investigates security breach involving patient records
Article URL: http://www.sfgate.com/health/article/SF-General-investigates-security-breach-involving-6119924.php

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150305-02	VA Corporate Data Center Operations / Austin	TX	1/7/2015	Electronic	Government/Military	Yes - Published #	7,029

VA Corporate Data Center Operations/Austin Information Technology Center TX Healthcare Provider 7029 01/07/2015 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: VA Corporate Data Center Operations / Austin Information Technology 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
ITRC20150305-01	Marketing Clique	TX	2/20/2015	Electronic	Business	Yes - Published #	8,700

Marketing Clique TX Health Plan 8700 02/20/2015 Unauthorized Access/Disclosure Other No

Attribution 1 Publication: hhs.gov Author:
Article Title: Marketing Clique
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
ITRC20150304-03	Fuse Energy / Percheron LLC	TX	2/23/2015	Electronic	Business	Yes - Unknown #	Unknown

On January 15, 2015, an unknown individual broke into Percheron's facility and stole several items, including a computer hard drive that contained certain tax forms. Our client believes that these tax forms contained personally identifiable information, including the names, social security numbers, addresses, and telephone numbers of Fuse Energy's lessors. The hard drive was not password protected, and the data it contained was not encrypted. However, the lessors' information can only be accessed by opening and searching through the individual tax forms stored on the hard drive.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Percheron LLC
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/percheron-20150223.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150304-02	Mandarin Oriental Hotel Group	NY	3/4/2015	Electronic	Business	Yes - Unknown #	Unknown

In response to questions from KrebsOnSecurity, upscale hotel chain Mandarin Oriental Hotel Group today confirmed that its hotels have been affected by a credit card breach. Reached for comment about reports from financial industry sources about a pattern of fraudulent charges on customer cards that had all recently been used at Mandarin hotels, the company confirmed it is investigating a breach. (CA = 2,835 residents)

Attribution 1 Publication: krebsonsecurity.com / CA AG's office / Author:
Article Title: Credit Card Breach at Mandarin Oriental
Article URL: http://krebsonsecurity.com/2015/03/credit-card-breach-at-mandarian-oriental/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150304-01	Xtra Mile Ambulance Service Company	TX	3/3/2015	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

State investigators are working to find out how hundreds of medical documents ended up in a dumpster at a storage facility in McAllen. The medical files contain personal information including Social Security numbers, addresses and bank account numbers. A CHANNEL 5 NEWS viewer found the files piled up in a dumpster at a storage facility. Many of the files appeared to be records from the Xtra Mile Ambulance Service Company. The company is no longer in business.

Attribution 1 Publication: phiprivacy.net / KRGV.com Author:
Article Title: State Investigates After Medical Files Found in Dumpster
Article URL: http://www.krgv.com/news/local-news/State-Investigates-After-Medical-Files-Found-in-Dumpster/31596764

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150303-08	Piedmont Advantage Credit Union	NC	3/2/2015	Electronic	Banking/Credit/Financial	Yes - Published #	46,000

North Carolina-based Piedmont Advantage Credit Union is notifying an undisclosed number of individuals that one of its laptops containing personal information – including Social Security numbers – cannot be located. UPDATE: According to a Piedmont Advantage Credit Union statement emailed to SCMagazine.com on Monday, "To alert its entire membership of 46,000, Piedmont Advantage mailed materials regarding the situation, the Kroll monitoring services and information on identify theft prevention."

Attribution 1 Publication: Scmagazine.com Author:
Article Title: North Carolina credit union notification says laptop containing data missing
Article URL: http://www.scmagazine.com/north-carolina-credit-union-notification-says-laptop-containing-data-missing/article/4011

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150303-07	Socorro Independent School District	TX	2/27/2015	Electronic	Educational	Yes - Unknown #	Unknown

The Socorro Independent School District spent $8,000 this weekend, cleaning up a number of Eastlake High computers. A student downloaded malware, or a malicious program to the school's computer system. After spending the weekend checking 1,000 computers, they found out he had only infected 16. Reyna said he was attempting to copy log-ins and passwords, with the intent of identify theft. The student was arrested and charged with breach of computer systems.

Attribution 1 Publication: databreaches.net / KVIA.com Author:
Article Title: Socorro ISD spends thousands after student downloads malicious program to Eastlake High computers
Article URL: http://www.kvia.com/news/socorro-isd-spends-thousands-after-student-hacks-eastlake-high-computers/31439278

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150303-06	Benecard Services, Inc.	NJ	2/28/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A class action lawsuit filed Feb. 26 claims prescription benefit company Benecard Services Inc., which has an office in Mechanicsburg, failed to notify former employees and customers of a recent data breach. At this point, Benecard believes the breach only impacts employees via a breach involving payroll records, but as the forensic investigation is not complete, it's not yet known whether any patients may have had their information breached.

Attribution 1 Publication: pennlive.com Author:
Article Title: Benecard employees say fraudulent tax returns filed through data breach
Article URL: http://www.pennlive.com/midstate/index.ssf/2015/02/benecard_employees_say_fraudul.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150303-05	Pioneer Bank	NY	3/2/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Pioneer Bank over the weekend alerted some of its customers that an employee's laptop stolen Jan. 26 contained "secured personal information of certain customers, including names, social security numbers, street addresses, and account and debit card numbers."

Attribution 1 Publication: timesunion.com / databreaches.net Author:
Article Title: Stolen Pioneer bank laptop contained some customers' data
Article URL: http://blog.timesunion.com/business/stolen-pioneer-bank-laptop-contained-some-customers-data/64014/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150303-04	Ziprick & Cramer LLP	CA	2/27/2015	Electronic	Business	Yes - Unknown #	Unknown

Unfortunately, on or around January 25, 2015, our firm was the victim of a single cyberattack, by a relatively new variant of a Cryptolocker-type virus (which is a fairly sophisticated form of ransomware, which is apparently being used by criminals around the world). It infected one of our workstations (with the virus encrypting data on the workstation), and then traveled to the in-house server where data was also encrypted on shared folders (collectively, the "Computer"). Accordingly, we are sending this notification letter to all clients for whom we had any data on the Computer.

Attribution 1 Publication: CA AG's office Author:
Article Title: Ziprick & Cramer LLP
Article URL: https://oag.ca.gov/system/files/LT%20Clients%20Sample%20w%20How%20To_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150303-03	Perspectives.org	IL	1/12/2015	Electronic	Educational	Yes - Unknown #	Unknown

As you may know, the Perspectives National Office has been investigating a breach of online security, which led us to temporarily close down payment options on the Perspectives website over the last few weeks. I first want to acknowledge how frustrating this has been for everyone including students, coordinators and other team members, especially as it came right in the middle of spring registrations – one of our busiest times of the year.

Attribution 1 Publication: CA AG's office Author:
Article Title: Perspectives.org
Article URL: https://secure.perspectives.org/breach-faq - a1

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150303-02	Toys "R" Us	NJ	1/29/2015	Electronic	Business	Yes - Unknown #	Unknown

Unnamed attackers attempted to gain access to some Toys“R”Us reward program members' profiles in January, prompting the company to send email notifications and request users change their passwords.

Attribution 1 Publication: scmagazine.com / CA AG's office Author:
Article Title: Attempts made to access Toys"R"Us reward program profiles
Article URL: http://www.scmagazine.com/attacks-attempt-to-access-rewardsrus-accounts/article/401160/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150303-01	Blue Cross Blue Shield - Minnesota	MN	3/3/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A nurse with a history of narcotics theft illegally accessed a state database that contains prescription drug records for 1 million Minnesotans, all under the supervision of government entities that cost taxpayers hundreds of millions of dollars annually.

Attribution 1 Publication: minnesota.cbslocal.com / phiprivacy.net Author: Esme Murphy
Article Title: Blue Cross Blue Shield Nurse Accused Of Illegally Accessing Patient Records
Article URL: http://minnesota.cbslocal.com/2015/03/02/blue-cross-blue-shield-nurse-accused-of-illegally-accessing-patient-records

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150302-12	Uber	CA	3/2/2015	Electronic	Business	Yes - Published #	50,000

Uber announced last week (Feb. 27) that the data of roughly 50,000 drivers may have been impacted in a security breach, but the car-hailing service company failed to report the information to drivers for five months after learning of the incident.

Attribution 1 Publication: pymnts.com / CA AG's office Author:
Article Title: UBER’S DRIVER DATA BREACH HIDDEN FOR FIVE MONTHS
Article URL: http://www.pymnts.com/news/2015/ubers-driver-databreach-hidden-for-five-months/ - .VPT7ifnF_rw

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150302-11	CP Franchising / Cruise Planners	FL	2/4/2015	Electronic	Business	Yes - Unknown #	Unknown

CP Franchising is committed to providing excellent travel experiences, and we are committed to the privacy and security of our clients. As part of this commitment, we are providing you this notice regarding potential unauthorized access to your information. You may have previously received an email notification from us indicating that your information may have been compromised. We are now sending this notification with more detailed information for your consideration. (509 NH residents)

Attribution 1 Publication: CA AG's office / MD AG's office Author:
Article Title: CP Franchising
Article URL: https://oag.ca.gov/system/files/CP%20Franchising%20-%20client%20notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150302-10	Natural Grocers	CO	3/2/2015	Electronic	Business	Yes - Unknown #	Unknown

Sources in the financial industry tell KrebsOnSecurity they have traced a pattern of fraud on customer credit and debit cards suggesting that hackers have tapped into cash registers at Natural Grocers locations across the country. The grocery chain says it is investigating “a potential data security incident involving an unauthorized intrusion targeting limited customer payment card data.”

Attribution 1 Publication: esecurityplanet.com Author: Jeff Goldman
Article Title: Natural Grocers Hacked
Article URL:

Attribution 2 Publication: krebsonsecurity.com Author: Brian Krebs
Article Title: Natural Grocers Investigating Card Breach
Article URL: http://krebsonsecurity.com/2015/03/natural-grocers-investigating-card-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150302-09	Suburban Lung Associates / FileFax Inc.	IL	2/26/2015	Paper Data	Medical/Healthcare	Yes - Published #	2,984

A massive breach of medical records containing confidential personal information has prompted both federal and state investigations. It all started when CBS 2 Investigator Dave Savini got a tip about what a dumpster diver found in the trash.

Attribution 1 Publication: chicago.cbslocal.com / phiprivacy.net Author: Dave Savini
Article Title: 2 Investigators: Medical Files With Personal Info Found In Dumpster
Article URL: http://chicago.cbslocal.com/2015/02/25/2-investigators-medical-files-with-personal-info-found-in-dumpster/

Attribution 2 Publication: databreaches.net Author:
Article Title: Illinois AG sues records storage company FileFax for dumping thousands of Suburban Lung Associates’ patients’ records
Article URL: http://www.databreaches.net/illinois-ag-sues-records-storage-company-filefax-for-dumping-thousands-of-suburban-lu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150302-06	Medical College of Wisconsin	WI	3/1/2015	Electronic	Medical/Healthcare	Yes - Published #	400

The Medical College of Wisconsin is contacting hundreds of people after a patient privacy breach. A spokesperson says a document containing private information on approximately 400 patients and a laptop with information on one patient were stolen. It happened when somebody broke into a doctor's car.The Medical College says no social security numbers or addresses were stolen and issued the following statement:

Attribution 1 Publication: phiprivacy.net / cbs58.com Author: Michele McCormack
Article Title: Security breach at Medical College of Wisconsin
Article URL: http://www.cbs58.com/story/28224655/security-breach-at-medical-college-of-wisconsin

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150302-05	Home Respiratory Care	CA	1/25/2015	Electronic	Medical/Healthcare	Yes - Published #	1,285

Diana S. Guth DBA Home Respiratory Care CA Healthcare Provider 1285 01/28/2015 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Home Respiratory 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
ITRC20150302-04	South Sunflower County Hospital	MS	2/4/2015	Paper Data	Medical/Healthcare	Yes - Published #	19,000

South Sunflower County Hospital MS Healthcare Provider 19000 02/04/2015 Improper Disposal Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: South Sunflower County 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
ITRC20150302-03	**Pathway to Hope**	FL	2/12/2015	Electronic	Medical/Healthcare	Yes - Published #	**600**

Pathway to Hope FL Healthcare Provider 600 02/12/2015 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Pathway to Hope
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
ITRC20150302-02	**Hunt Regional Medical Partners**	TX	2/18/2015	Paper Data	Medical/Healthcare	Yes - Published #	**3,000**

Hunt Regional Medical Partners Family Practice at Westlake is notifying patients that a warehouse storing patient records was vandalized January 16-17, 2015.

Attribution 1 Publication: hhs.gov Author:
Article Title: Hunt Regional Medical Partners Family Practice at Westlake notifies patients that records were stolen from warehouse
Article URL: http://www.phiprivacy.net/tx-hunt-regional-medical-partners-family-practice-at-westlake-notifies-patients-that-records-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150302-01	**Office of Raymond Mark Turner, MD**	NV	2/26/2015	Electronic	Medical/Healthcare	Yes - Published #	**2,153**

Raymond Mark Turner, M.D. NV Healthcare Provider 2153 02/26/2015 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Raymond Mark Turner, 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
ITRC20150225-04	**Urban Institute's National Center for Charitable**	DC	2/24/2015	Electronic	Business	Yes - Unknown #	**Unknown**

The Urban Institute's National Center for Charitable Statistics (NCCS) recently discovered that an unauthorized party or parties gained access to the Form 990 Online and e-Postcard filing systems for nonprofit organizations. The intruder or intruders retrieved email addresses, usernames, passwords, first and last names, IP addresses, phone numbers, and addresses and names of nonprofits.

Attribution 1 Publication: databreaches.net Author:
Article Title: National Center for Charitable Statistics Discovers Unauthorized Access to Form 990 and e-Postcard Filing Systems for Nonpr
Article URL: http://www.databreaches.net/national-center-for-charitable-statistics-discovers-unauthorized-access-to-form-990-and-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150225-03	**Anthem, Inc. (non-customers) - Blue Cross Blue**	IN	2/25/2015	Electronic	Medical/Healthcare	Yes - Published #	**8,800,000**

On Tuesday, an Anthem, Inc spokesperson stated that anywhere from 8.8 million to 18.8 million non-customers could be impacted by the previously announced Anthem data breach, according to a Reuters report. Earlier this month, Anthem, Inc.announced that outside hackers breached a data base containing the personally identifiable information (PII) of approximately 80 million individuals. Just this week Anthem revised that number to 78.8 million compromised records.

Attribution 1 Publication: healthITsecurity.com / Reuters.com Author: Stephanie Reardon
Article Title: Anthem Data Breach May Impact 8.8 to 18.8M Non-Customers
Article URL: http://healthitsecurity.com/2015/02/25/anthem-data-breach-may-impact-8-8-to-18-8-m-non-customers/ - more-'

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150225-02	**Kaplan University**	IA	2/11/2015	Electronic	Educational	Yes - Unknown #	**Unknown**

On June 4, 2014, the UV A OIG/CID alerted Kaplan that it was the victim of theft involving a former Kaplan University employee and the personal information of some of its students. Kaplan immediately began to investigate after learning about this incident, and has devoted considerable time and effort to determine what information the hardcopy documents contained. We can confirm that those documents contained the resident's full name and Social Security number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Kaplan University
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/kaplan-university-20150211.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150225-01	**KSI Trading Corporation / TriNet**	VA	2/20/2015	Electronic	Business	Yes - Published #	**641**

Please be advised that on or about February 9, 2015, in connection with the administration of TriNet's services to its customer KSI Trading Corporation, an email attaching documentation containing personal information ofKSI's worksite employees was inadvertently sent to an employee at one ofTriNet's customers. The personal information included the names and social security numbers of KSI's employees.

Attribution 1 Publication: NH AG's office Author:
Article Title: KSI Trading Corporation / TriNet
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/ksi-trading-20150220.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150224-04	**Office of Jeb Bush**	FL	2/13/2015	Electronic	Business	Yes - Published #	**13,000**

Earlier this week, former Florida governor Jeb Bush released online a cache of emails sent and received by his personal email address during his time in office. His attempt at transparency turned sour after it was realized that some emails contained personally identifiable information of Floridians, including social security numbers, names, and dates of birth. (333,000 emails)

Attribution 1 Publication: fortune.com Author:
Article Title: Jeb Bush exposed 13,000 social security numbers. Here's where they were hiding
Article URL: http://fortune.com/2015/02/13/jeb-bush-social-security-numbers/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150224-03	**Lime Crime**	CA	2/21/2015	Electronic	Business	Yes - Unknown #	**Unknown**

The website for the vegan makeup company Lime Crime, whose wares are sold by Urban Outfitters and Nasty Gal, among others, admitted they'd been hacked earlier this week and that customer information has been compromised. But customers are up in arms over the way the site handled telling them that – or not telling them, as the case may be.

Attribution 1 Publication: databreaches.net / Jezebel / CA AG's of Author:
Article Title: Lime Crime's Website Is Hacked, Customer Information Stolen
Article URL: http://jezebel.com/lime-crimes-website-is-hacked-customer-information-sto-1686744501

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150224-02	**Bulk Reef Supply**	MN	2/21/2015	Electronic	Business	Yes - Unknown #	**Unknown**

We want to express our sincere regret to the customers of Bulk Reef Supply whose personal information was stolen from our website server. BulkReefSupply.com (“BRS”) learned of a data security incident caused by an outside hacker intrusion to its website. While we are continuing to investigate this incident, we do know that some customer data for customers who logged into the website from July 30, 2014 until January 30, 2015 may have been compromised.

Attribution 1 Publication: databreaches.net Author:
Article Title: Bulk Reef Supply web site compromised between July 2014 – January 2015
Article URL: http://www.databreaches.net/bulk-reef-supply-web-site-compromised-between-july-2014-january-2015/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150224-01	AAAA TV	CO	2/24/2015	Paper Data	Business	Yes - Unknown #	Unknown

Investigative reporter Heidi Hemmat was at the store located on South Holly Street Monday morning after receiving a tip that said the owner of the store was throwing away customers' personal information in a dumpster behind the store. Hemmat discovered hundreds of paper receipts and documents containing customers' personal information, bank accounts and credit card numbers. The owner of the store, Muhammed Murib, confronted Hemmat after she jumped in the dumpster and looked through the documents.

Attribution 1 Publication: databreaches.net Author:
Article Title: Dumpster confrontation; FOX31 investigator finds customers' personal info
Article URL: http://www.databreaches.net/watch-dumpster-confrontation-fox31-investigator-finds-customers-personal-info/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150223-03	Planned Parenthood Southwest Ohio	OH	2/5/2015	Paper Data	Medical/Healthcare	Yes - Published #	5,000

Planned Parenthood Southwest Ohio OH Healthcare Provider 5000 02/05/2015 Improper Disposal Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Planned Parenthood Southwest Ohio
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
ITRC20150223-02	Office of Arturo Tomas	IL	2/9/2015	Paper Data	Medical/Healthcare	Yes - Published #	680

Tomas, Arturo IL Business Associate 680 02/09/2015 Loss Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Arturo Tomas
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
ITRC20150223-01	Lone Star Circle of Care	TX	2/20/2015	Electronic	Medical/Healthcare	Yes - Published #	8,700

A data breach at Lone Star Circle of Care has compromised the personal information of 8,700 people, including 6,300 patients, officials said Friday. The breach was discovered Jan. 9 after a backup file containing mostly names, addresses, phone numbers, and in some cases, birth dates, was improperly placed on Lone Star's website by the company that designed, maintained and secured the website. The data had been posted for nearly six months before Lone Star realized what had happened, officials said.

Attribution 1 Publication: phiprivacy.net / statesman.com Author:
Article Title: Data breach at Lone Star Circle of Care affects 8,700
Article URL: http://www.statesman.com/news/news/data-breach-at-lone-star-circle-of-care-affects-87/nkFyY/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150220-01	Office of Cathrine Steinborn DDS	CA	2/18/2015	Electronic	Medical/Healthcare	Yes - Published #	3,224

Dr. Cathrine Steinborn, DDS, is providing notice of a recent office theft which may affect the security of patient and responsible party personal and protected health information. On January 5, 2015, Dr. Steinborn's office was burglarized and a server containing patient and responsible party information was stolen. The burglary was immediately reported to Santa Clara Police Department.

Attribution 1 Publication: CA AG's office / website / hhs.gov Author:
Article Title: https://oag.ca.gov/system/files/Press%20release%20and%20website%20notice_0.pdf?
Article URL: Office of Cathrine Steinborn DDS

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150219-02	trueEX	NY	2/17/2015	Electronic	Business	Yes - Unknown #	Unknown

Recently, it was discovered that a single employee's email inbox had been improperly accessed by an unauthorized third party. Our records indicate that your name, social security number and 2013 compensation may have been compromised as part of this incident

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150219-01	University of Maine	ME	2/18/2015	Electronic	Educational	Yes - Published #	941

A data breach discovered last week has exposed the personal information of more than 900 current and former University of Maine students, the university announced Wednesday.

Attribution 1 Publication: databreaches.net / Scmagazine.com Author:
Article Title: UMaine probing data breach affecting more than 900
Article URL: http://www.databreaches.net/umaine-probing-data-breach-affecting-more-than-900/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-14	Otsuka America, Inc.	CA	1/29/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

This letter is to inform you of a privacy incident affecting residents of your state. We have been hired by Otsuka America, Inc. to notify and provide identity theft protection to persons whose personal information was stored on a server backup tape that was included in a stolen package. The theft occurred while the package - which did not contain any indication of what was inside - was in transit from their San Francisco office to their offsite storage facility in Portland, Oregon.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Otsuka America, Inc.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/otsuka-america-20150129.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-13	Operon Resource Management	MA	1/21/2015	Paper Data	Business	Yes - Unknown #	Unknown

The breach of security occurred on January 4, 2015 when the vehicle of an Operon Resource Management staff member was stolen from her residence. Locked inside the vehicle was a briefcase that contained personal employee records in paper form. These records included employment applications, contact information, skill and training assessments, resumes, W-4 forms containing social security numbers, and voided checks with bank account information (for direct deposit set up purposes).

Attribution 1 Publication: NH AG's office Author:
Article Title: Operon Resource Management
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/operon-20150121.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-12	Harvard Pilgrim Health Care	MA	1/21/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On December 1 0, 2014, a Harvard Pilgrim laptop was stolen from the Massachusetts home of a Harvard Pilgrim employee between the hours of 1 Oam and 1 pm. When the employee returned home and discovered the theft, she called the police and filed a police report. On the same day,the employee notified her supervisor at Harvard Pilgrim who in tum notified Harvard Pilgrim's Office of Information Security.

Attribution 1 Publication: NH AG's office Author:
Article Title: Harvard Pilgrim Health Care
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/harvard-pilgrim-health-care-20150121.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-11	Ameriprise Financial Services, Inc.	MN	2/6/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

This letter is for the purpose of notifying your office that Ameriprise Financial Services, Inc. had a data breach incident involving the theft of information for one (1) Ameriprise client who is a resident of New Hampshire. Specifically, an advisor office was recently broken into and the file cabinets forced open. The file cabinets contained the advisor's client files. Client files contain copies of financial documents, which can include client name, date of birth, medical information, driver's license, Social Security and account numbers.

Attribution 1 Publication: NH AG's office Author:
Article Title: Ameriprise Financial Services, Inc.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/ameriprise-financial-services-20150206.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-10	Intuit /TurboTax	CA	2/5/2015	Electronic	Business	Yes - Unknown #	Unknown

We've identified what appears to be unauthorized access to your TurboTax account on or around January 29, 2015. As a result, criminals may have obtained information contained on your prior year tax returns. This letter details steps we've taken to help protect you and suggestions on how to protect yourself in the future. Please feel free to call us if you have questions. We are here to help.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-09	Philadelphia Common Pleas Court	PA	2/16/2015	Paper Data	Government/Military	Yes - Unknown #	Unknown

Documents with personal information, such as social security numbers and signatures, were found strewn all over the Grays Ferry section of Philadelphia on Tuesday.

Attribution 1 Publication: databreaches.net / ABC news Author:
Article Title: Hundreds of court documents found scattered in Philadelphia
Article URL: http://www.databreaches.net/pa-hundreds-of-court-documents-found-scattered-in-philadelphia/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-08	BigFishGames.com	WA	2/11/2015	Electronic	Business	Yes - Unknown #	Unknown

I am writing to inform you of an incident we self-discovered on January 12, 2015, involving the theft of payment information from our online stores. An unknown criminal installed malware on the billing and payment pages of our websites that appears to have intercepted customer payment information. Your information may have been affected if you entered new payment details on our websites (rather than using a previously saved profile) for purchases between December 24, 2014 and January 8, 2015. Your name, address, and payment card information, including the card number, expiration date, and CVV2 code, may have been among the information accessed.

Attribution 1 Publication: CA AG's office Author:
Article Title: Big Fish
Article URL: https://oag.ca.gov/system/files/BFG%20-%20MULTI-STATE%20NOTIFICATION%20LETTER_Proof_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-07	State of Franklin Healthcare Associates	TN	2/13/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Tennessee-based State of Franklin Healthcare Associates (SoFHA) has notified all employees that their personal information was accessed during a security breach at the company's third party payroll vendor, and some if has already been used to file fraudulent tax returns.

Attribution 1 Publication: Scmagazine.com / beckershospitalrevie Author: Adam Greenberg
Article Title: Tennessee healthcare group notifies employees of payroll breach
Article URL: http://www.scmagazine.com/tennessee-healthcare-group-notifies-employees-of-payroll-breach/article/398240/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-06	Kaiser Permanente Hawaii	HI	2/14/2015	Paper Data	Medical/Healthcare	Yes - Published #	6,600

On Wednesday, January 7, 2015, a box of documents being transported to storage on Oahu via contracted courier from Kaiser Permanente's Kona Medical Office, spilled from the courier's moving vehicle. Swift action by Kaiser Permanente employees allowed the retrieval of many of the documents, but unfortunately, not all were recovered.

Attribution 1 Publication: phiprivacy.net / Kaiser website Author:
Article Title: Kaiser Permanente Hawaii
Article URL: http://www.phiprivacy.net/kaiser-permanente-notifies-hawaii-members-of-pharmacy-records-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150217-05	Office of Ronald D. Garrett-Roe, MD	TX	2/17/2015	Electronic	Medical/Healthcare	Yes - Published #	1,600

Ronald D. Garrett-Roe, MD TX Healthcare Provider 1600 02/28/2014 - 10/31/2014 Hacking/IT Incident Desktop Computer (2015 post date)

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Ronald D. Garrett-Roe, 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
ITRC20150217-04	North Dallas Urogynecology PLLC	TX	2/17/2015	Electronic	Medical/Healthcare	Yes - Published #	678

North Dallas Urogynecology, PLLC. TX Healthcare Provider 678 12/04/2014 - 12/04/2014 Theft Laptop (2015 post date)

Attribution 1 Publication: hhs.gov Author:
Article Title: North Dallas Urogynecology 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
ITRC20150217-03	National Pain Institute	FL	2/17/2015	Electronic	Medical/Healthcare	Yes - Published #	500

National Pain Institute FL Healthcare Provider 500 07/13/2013 - 08/13/2013 Improper Disposal Desktop Computer, Laptop (2015 post date)

Attribution 1 Publication: hhs.gov Author:
Article Title: National Pain Institute
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
ITRC20150217-02	mdINR LLC	FL	2/17/2015	Electronic	Medical/Healthcare	Yes - Published #	1,859

mdINR LLC FL Healthcare Provider 1859 11/03/2014 - 11/03/2014 Unauthorized Access/Disclosure Email (2015 post date)

Attribution 1 Publication: hhs.gov Author:
Article Title: mdINR 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
ITRC20150217-01	Office of David E. Hansen, DDS PS	WA	2/17/2015	Electronic	Medical/Healthcare	Yes - Published #	2,000

David E. Hansen DDS PS WA Healthcare Provider 2000 05/10/2014 - 05/10/2014 Theft Other Portable Electronic Device, Paper/Films (2015 post date)

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of David E. Hansen, DDS PS
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=624FA3CBAA47E8308187183DD69EACE5.worker1

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150213-06	Blue Sky Casino / French Lick Resort	IN	2/6/2015	Electronic	Business	Yes - Published #	54,624

The purpose of this letter is to inform you about a payment card incident that was identified by French Lick Resort. On January 19, 2015 we learned that a hacker installed malware (a software credit card scraping device) on some of our card payment devices, which compromised the security of the credit card systems that we use for purchases at our Resort by guests, visitors, and our associates.

Attribution 1 Publication: indystar.com Author:
Article Title: Indiana's top 10 data breaches so far this year
Article URL: http://www.indystar.com/story/money/2015/07/18/indianas-top-10-data-breaches-so-far-year/30360027/

Attribution 2 Publication: NH AG's office Author:
Article Title: Blue Sky Casino / French Lick Resort
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/french-lick-resort-20150131.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150213-05	Visteon Corporation / Fidelity Investments	MI	1/16/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Pursuant to RSA 359-C:20 and on behalf of Visteon Corporation, we are writing to notify you of an unauthorized disclosure of personal information. Fidelity is the record keeper and administrative services provider for the Visteon Supplemental Executive Retirement Plan (SERP). On December 1, 2014, information about twenty-eight participants in the Visteon SERP was inadvertently included in a report that was sent by Fidelity to another Fidelity client firm.

Attribution 1 Publication: NH AG's office Author:
Article Title: Visteon Corporation / Fidelity Investments
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/fidelity-20150116.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150213-04	Dartmouth-Hitchcock Medical Center	NH	1/28/2015	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

I write to notify you of a data privacy incident at Dartmouth-Hitchcock ("D-H") that has affected the security of personal information of one New Hampshire resident. D-H's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission. On November 23, 2014, D-H discovered that, as a result of a phishing incident, one D-H employee user account had unauthorized activity in the Employee Self Service Direct Deposit Payroll system. D-H immediately commenced an investigation of the incident to examine the extent of the unauthorized activity.

Attribution 1 Publication: NH AG's office Author:
Article Title: Dartmouth-Hitchcock Medical Center
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/dartmouth-hitchcock-20150210.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150213-03	Citibank, N.A.	NY	1/23/2015	Paper Data	Banking/Credit/Financial	Yes - Unknown #	Unknown

On behalf of Citibank, N .A. ("Citi"), I am writing to inform your that it was recently discovered that the addresses listed for a small number of accounts contained the
accountholders' social security numbers in one of the address lines. We determined that no other personal information was exposed, and we are unaware of any harm caused by this exposure.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Citibank, N.A.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/citi-20150120.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150213-02	**Citibank, N.A.**	NY	1/27/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

On behalf of Citibank, N.A. ("Citi"), I am writing to inform you about an event that took place on December 4, 2014 in which limited personal information maintained by Citi relating to one New Hampshire resident was improperly accessed by a Citibank employee. As a result of our investigation, this person is no longer working at Citibank. (Sioux Falls, SD)

Attribution 1 Publication: NH AG's office Author:
Article Title: Citibank, N.A.
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/citibank-20150127.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150213-01	**Power Plant Services (Alin Machining Company)**	IL	1/13/2015	Electronic	Business	Yes - Unknown #	**Unknown**

On December 10, 2014, Alin Machining Company Inc. (d/b/a Power Plant Services) learned that an independent contractor may have misused personal employee information for a very small group of Power Plant Services personnel between November 7, 2014 and December 4, 2014. The types of information that were the subject of this incident include: • Name • Address • Social Security Number • Bank Account Number

Attribution 1 Publication: NH AG's office Author:
Article Title: Power Plant Services (Alin Machining Company)
Article URL: http://doj.nh.gov/consumer/security-breaches/documents/alin-machining-company-inc-dba-power-plant-services-2015

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150210-04	**Utah State University**	UT	2/7/2015	Electronic	Educational	Yes - Published #	**347**

A Utah State University staff member accidentally sent an email message Thursday, Feb. 5, containing 347 individual names and social security numbers to a group of USU student Veterans. The email included social security numbers and names, but no other personal information. The email went to 1,033 people.

Attribution 1 Publication: databreaches.net Author:
Article Title: Email gaffe exposes 347 Utah State University students' Social Security numbers
Article URL: http://www.databreaches.net/email-gaffe-exposes-347-utah-state-university-students-social-security-numbers/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150210-03	**Mesa del Sol Golf Club**	AZ	2/7/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Yuma County sheriff's deputies are investigating the fraudulent use of credit card numbers stolen from the Mesa del Sol Golf Club clubhouse in January.
Sheriff's spokesman Alfonso Zavala said Thursday there are at least 41 known unauthorized transactions stemming from the breach, though he didn't know the number of cards they were charged to.

Attribution 1 Publication: yumasun.com Author: Blake Herzog
Article Title: Credit card data stolen from golf facility
Article URL: http://www.yumasun.com/news/credit-card-data-stolen-from-golf-facility/article_936ff6b0-af51-11e4-aca0-2fbd5e8f35f0.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150210-02	**Shorter University**	GA	2/8/2015	Paper Data	Educational	Yes - Unknown #	**Unknown**

The September 2014 theft of student files from Shorter University could be the source of problems for two Rome women who say they are the victims of fraudulent tax returns.

Attribution 1 Publication: northwestgeorgianews.com / databreach Author: Jeremy Stewart
Article Title: Shorter students claim to be victims of identity theft
Article URL: http://www.northwestgeorgianews.com/rome/news/local/shorter-students-claim-to-be-victims-of-identity-theft/article_f

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150210-01	**Jefferson National Parks Association**	MO	2/9/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Jefferson National Parks Association announced on Friday that malware was identified on point-of-sale (POS) devices at two gift shops at the Gateway Arch in St. Louis, and payment card information may have been compromised for anyone who used their payment cards at those terminals.

Attribution 1 Publication: scmagazine.com Author: Adam Greenberg
Article Title: POS malware threatens payment cards used at Gateway Arch shops
Article URL: http://www.scmagazine.com/pos-malware-threatens-payment-cards-used-at-gateway-arch-shops/article/397201/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150209-02	**Phoenix House**	NY	2/5/2015	Electronic	Business	Yes - Published #	**2,000**

On December 22, 2014, Phoenix House learned that, on December 19. 2014, a consultant hired to perform payroll activities for us appears to have made unauthorized changes in our electronic payroll systems hosted by third parties. Upon learning this, we immediately removed the consultant's access to the systems at issue and conducted an investigation to determine what infonnation may have been changed.

Attribution 1 Publication: CA AG's office Author:
Article Title: Phoenix House
Article URL: https://oag.ca.gov/system/files/PHOENIX%20HOUSE_%20INDIVIDUAL%20NOTIFICATION%20VERSION%201_WPP-RE

Attribution 2 Publication: scmagazine.com Author: Adam Greenberg
Article Title: Phoenix House notifies current and former employees of potential data incident
Article URL: http://www.scmagazine.com/phoenix-house-notifies-current-and-former-employees-of-potential-data-incident/article/3

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150209-01	**Rainier Surgical Inc.**	TX	2/9/2015	Paper Data	Medical/Healthcare	Yes - Published #	**4,920**

Rainier Surgical, Incorporated TX Healthcare Provider 4920 11/18/2014 - 11/18/2014 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Rainier Surgical 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
ITRC20150205-02	**Boston Baskin Cancer Foundation**	MA	2/3/2015	Electronic	Medical/Healthcare	Yes - Published #	**56,694**

Patients got a letter in the mail, saying a robber broke into a clinic employee's home back in December and stole a hard drive with patient information on it. The hard drive had things like Social Security numbers, names, addresses, and birth dates.

Attribution 1 Publication: databreaches.net / OCR Author:
Article Title: Follow-up: Boston Baskin Cancer improved data security safeguards following breach
Article URL:

Attribution 2 Publication: phiprivacy.net /wreg.com / hhs.gov Author:
Article Title: Boston Baskin Cancer Foundation patients and employees notified of stolen hard drive
Article URL: http://www.phiprivacy.net/tn-boston-baskin-cancer-foundation-patients-and-employees-notified-of-stolen-hard-drive/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150205-01	**Anthem, Inc. - Customers**	IN	2/4/2015	Electronic	Medical/Healthcare	Yes - Published #	**78,800,000**

Health insurer Anthem Inc. has suffered a massive data breach after hackers gained access to a corporate database reportedly containing personal information on as many as 80 million of the health insurer's current and former U.S. customers and employees. "Anthem was the target of a very sophisticated external cyber attack," says Joseph R. Swedish, president and CEO of Indianapolis, Ind.-based Anthem Inc., on a dedicated Anthem Facts website that includes a FAQ relating to the breach. "These attackers gained unauthorized access to Anthem's IT system and have obtained personal information from our current and former members, such as their names, birthdays, medical IDs/social security numbers, street addresses, e-mail addresses and employment information, including income data," he said.

Attribution 1 Publication: healthinfosecurity.com / CA AG's office / Author: Mathew J. Schwartz
Article Title: Anthem Hit by Massive Data Breach
Article URL: http://www.healthcareinfosecurity.com/anthem-health-hit-by-massive-data-breach-a-7876?rf=2015-02-05-eh&utm_sour

Attribution 2 Publication: KrebsonSecurity Author:
Article Title: Data Breach at Health Insurer Anthem Could Impact Millions
Article URL: http://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150202-06	**Book2Park.com**	VA	2/2/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Last week, a new batch of credit card numbers [dubbed “Denarius“] went up for sale on Rescator[dot]cm, the cybercrime bazaar that earned infamy by selling tens of millions of cards stolen from Target and Home Depot. Multiple banks contacted by this author acquired a handful of cards from this new batch, and each of those financial institutions found the same pattern: All of the cards they bought had been issued to customers who recently made airport parking reservations at Book2Park.com.

Attribution 1 Publication: KrebsonSecurity.com Author: Brian Krebs
Article Title: Target Hackers Hit Third Parking Service
Article URL: http://krebsonsecurity.com/2015/02/target-hackers-hit-third-parking-service/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150202-05	**Liberty Tax Service**	CA	2/2/2015	Paper Data	Business	Yes - Unknown #	**Unknown**

A “large number” of documents were stolen Sunday from a business specializing in tax returns, potentially putting customers’ identities and finances at risk, according to the Sheriff’s Department. About 11:56 a.m. a burglar or burglars disabled the alarm at Liberty Tax Service, 27214 Base Line, and forced their way in, the Sheriff’s Department said in a statement. “The suspect(s) stole a large number of tax files and computer towers from inside the business,” the statement said. Clients’ names, addresses, Social Security numbers and other identifying information were listed on the stolen documents and hard drives.

Attribution 1 Publication: databreaches.net / Inland Valley Daily B Author: Greg Cappis
Article Title: Fraud risk for clients of Highland tax business after documents stolen
Article URL: http://www.sbsun.com/general-news/20150201/fraud-risk-for-clients-of-highland-tax-business-after-documents-stolen

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150202-04	**Greers Professional Fabricare Services**	VT	1/26/2015	Electronic	Business	Yes - Unknown #	**Unknown**

I am writing to you because of a recent security incident at Greers Professional Fabricare. Our server was breached and some credit card number were stolen, it appears that the card numbers and customer names were breached but no social security numbers or addresses were acquired. A forensic analysis has found and corrected the problem and we have added another layer of protection in order to prevent this from ever happening again. If you used a credit card at any one of our locations between April 1st 2014 and January 16th 2015 you might be affected.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150202-03	CICS Employment Services, Inc. - FBI notification	OR	1/9/2015	Electronic	Business	Yes - Unknown #	Unknown

We were recently notified by the Federal Bureau of Investigation (the FBI) that personal information we processed regarding an application you made for employment may have been accessed without authorization. This information included your name, address, date of birth and Social Security number. We do not know how or when the alleged unauthorized access may have occurred. The FBI's forensic examinations of relevant portions of our computer network, database and third party storage provider revealed no evidence of any compromise.

Attribution 1 Publication: CA AG's office Author:
Article Title: CICS Employment Services, Inc. - FBI notification
Article URL: https://oag.ca.gov/system/files/Notice_N095_v01_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150202-02	Umass Memorial Medical Group	MA	1/31/2015	Electronic	Medical/Healthcare	Yes - Published #	14,000

The UMass Memorial Medical Group is working with law-enforcement personnel after it learned a former employee allegedly accessed private patient billing information that contained credit card and debit card numbers, Social Security numbers, and birth dates, according to hospital personnel.

Attribution 1 Publication: phiprivacy.net / sentinelandenterprise.co Author:
Article Title: UMass Memorial data breach leaves 14,000 at risk
Article URL: http://www.sentinelandenterprise.com/breakingnews/ci_27431329/umass-memorial-data-breach-leaves-14-000-at

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150202-01	Senior Health Partners / Premier Home Health	NY	2/2/2015	Electronic	Medical/Healthcare	Yes - Published #	2,772

Senior Health Partners (SHP), a Healthfirst company, is today notifying approximately 2,700 of its members that a laptop and smartphone belonging to an assessment nurse employed by Premier Home Health ("Premier"), a business associate, were stolen from the nurse's apartment. On November 26, 2014, a laptop bag containing a laptop and smartphone was stolen from an assessment nurse who worked for Premier. The laptop was password-protected and encrypted; however, the encryption key was stolen with the laptop bag. The smartphone was neither password-protected nor encrypted. Premier notified SHP of the theft on December 10, 2014. SHP

Attribution 1 Publication: phiprivacy.net / SHP / hhs.gov Author:
Article Title: Senior Health Partners Provides Notice of Data Security Incident
Article URL: http://www.phiprivacy.net/senior-health-partners-provides-notice-of-data-security-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150130-01	Riverside County Regional Medical Center (RCRMC) #2	CA	1/30/2015	Electronic	Medical/Healthcare	Yes - Published #	7,925

An unencrypted laptop computer reported missing from Riverside County Regional Medical Center (RCRMC) in December might have contained the personal information of patients who received ophthalmology and dermatology services at the hospital between Jan. 26, 2012 and last Nov. 26.

Attribution 1 Publication: phiprivacy.net / abc7.com Author:
Article Title: Missing Riverside hospital laptop may have contained data of 7,900 patients
Article URL: http://abc7.com/news/missing-hospital-laptop-contained-data-of-7900-patients/496800/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150127-04	University of Chicago - Biological Sciences Division	IL	1/24/2015	Electronic	Educational	Yes - Published #	2,024

In a statement to DataBreaches.net, @MarxistAttorney reported that they got payroll information, employee IDs and a "substantial amount of information they didn't publicize." A copy of the url vulnerable to SQLi exploit was included in their statement.

Attribution 1 Publication: blog.credit.com Author:
Article Title: University of Chicago Data Breach Exposes Social Security Numbers
Article URL: http://blog.credit.com/2015/03/university-of-chicago-data-breach-exposes-social-security-numbers-110919/

Attribution 2 Publication: databreaches.net Author:
Article Title: U. Chicago hacked by Carbonic – claim (Updated)
Article URL: http://www.databreaches.net/u-chicago-hacked-by-teamcarbonic-claim/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150127-03	Harel Chiropractic	WI	1/26/2015	Electronic	Medical/Healthcare	Yes - Published #	3,000

Harel Chiropractic Clinic notified 3,000 patients Monday that some patient personal information may have been breached on Nov. 4, 2014, by an employee and a contract chiropractor. Clinic officials discovered the breach on Nov. 20.

Attribution 1 Publication: phiprivacy.net Author:
Article Title: Harel Chiropractic Clinic notifies 3,000 patients of breach
Article URL: http://www.phiprivacy.net/wi-harel-chiropractic-clinic-notifies-3000-patients-of-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150127-02	Lubbock Housing Authority	TX	1/20/2015	Electronic	Government/Military	Yes - Published #	1,100

Representatives of the Lubbock Housing Authority are asking anyone who filled out a Section 8 application to call their office, as personal information may have been breached. Mike Chapman, executive director, said because the program is so popular — and officials want the selection process to be fair — employees compile all the applicants into one spreadsheet and then do a random sort to place them in order on the waiting list. He compared the system to a lottery. He said the file mistakenly put on the website contained the applicants' whole Social Security numbers and estimated income, along with their names and addresses.

Attribution 1 Publication: datalossdb.org / lubbockonline.com / dat Author: Matt Dotray
Article Title: LHA mistakenly posts personal information, now offering credit monitoring
Article URL: http://lubbockonline.com/local-news/2015-01-21/lha-mistakenly-posts-personal-information-now-offering-credit-monit

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150127-01	California State University - Dominguez Hills	CA	1/20/2015	Electronic	Educational	Yes - Unknown #	Unknown

SUMMARY - 747 student email addresses and clear text passwords dumped on the internet

Attribution 1 Publication: datalossdb.org Author:
Article Title: California State University - Dominguez Hills
Article URL: http://datalossdb.org/incidents/14886-747-student-email-addresses-and-clear-text-passwords-dumped-on-the-internet

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150126-01	California Pacific Medical Center	CA	1/25/2015	Electronic	Medical/Healthcare	Yes - Published #	845

California Pacific Medical Center (CPMC) recently notified 844 patients of its discovery that a pharmacist employee may have accessed their records without a business or treatment purpose. CPMC first learned of the incident through a proactive audit of its electronic medical record system on October 10, 2014. The initial audit resulted in identification and notification of 14 individuals on October 21, 2014. Following its policy, CPMC terminated its relationship with the employee and broadened the investigation

Attribution 1 Publication: phiprivacy.net / CA AG's office Author:
Article Title: California Pacific Medical Center discovers employee was improperly accessing patient records for one year
Article URL: http://www.phiprivacy.net/california-pacific-medical-center-discovers-employee-was-improperly-accessing-patient-rec

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-14	Mount Pleasant Independent School District	TX	1/21/2015	Electronic	Educational	Yes - Published #	915

Personal information of approximately 915 present and former staff members of Mount Pleasant ISD may have been compromised between Jan. 18 and Jan. 21.

Attribution 1 Publication: dailytribune.net / databreaches.net Author: Gary Borders
Article Title: Data breach hits MPISD employees
Article URL: http://www.dailytribune.net/news/data-breach-hits-mpisd-employees/article_051ec5d0-a1d2-11e4-b1c7-afde4a6d4ed1.h

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-13	St. Peter's Health Partners	NY	1/23/2015	Electronic	Medical/Healthcare	Yes - Published #	5,117

St. Peter's Health Partners is warning of a possible data breach in its email system, following the theft of a manager's cellphone. Emails on the cellphone may have included patient information related to appointment schedules at St. Peter's Health Partner's Medical Associates, a large doctors' practice.

Attribution 1 Publication: scmagazine.com / healthitsecurity.com Author: Adam Greenberg
Article Title: Albany health system notifies more than 5,000 patients of data breach
Article URL: http://www.scmagazine.com/albany-health-system-notifies-more-than-5000-patients-of-data-breach/article/394364/

Attribution 2 Publication: timesunion.com / phiprivacy.net / Author: Claire Hughes
Article Title: St. Peter's Health Partners warns of possible data breach
Article URL: http://www.timesunion.com/news/article/St-Peter-s-Health-Partners-warns-of-possible-6035391.php

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-12	Xand Corporation	NY	1/23/2015	Electronic	Business	Yes - Published #	3,334

BA List at HHS.gov: Xand Corporation NY Business Associate 3334 02/02/2014 - 03/19/2014 Other Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Xand Corporation
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
ITRC20150123-11	TMA Practice Management Group	TX	1/23/2015	Electronic	Business	Yes - Published #	2,260

BA List at HHS.gov: TMA Practice Management Group TX Business Associate 2260 01/09/2014 - 03/14/2014 Improper Disposal, Loss Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: Texas Medical Association (TMA) Practice Management Group
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-10	Citibank, N.A.	NY	1/23/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Maryland AG update: We are writing to inform you that your account number for the above account was Included In Information sent by an employee to the employee's e-mail address. That employee's association with us has since terminated. The Information In the e-mail related to your account also included your name and certain balance information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Citibank, N.A.
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247040.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-09	Conference USA, Inc. (Blue Zebra)	TX	1/23/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: Conference USA, Inc. (the "Conference"), through its membership in the COC Men's Basketball LLC, a Delaware limited liability company (the "COC MB"), recently became aware of a security incident involving unauthorized access to the personal information of its men's college basketball officials on the website of one of the COC MB's contractors, Blue Zebra Spmis ("Blue Zebra"). A number of officials who had valid access to the Blue Zebra system used credentials that did not belong to them to access restricted pages containing the personal information of other officials, including such officials' names, addresses, birthdates and social security numbers, among other information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Conference USA, Inc. (Blue Zebra)
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248644.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-08	Cultivian Ventures, LLC	IN	1/23/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: On October 17, 2014, I became aware that one of my email accounts was compromised. I took action the same day to secure the account, and started working with our counsel to investigate the situation. The compromised email account has been used in the transmission and storage of documents on behalf of Cultivian Ventures, LLC ("Cultivian") clients. The information contained in the documents stored on the compromised email account may include names, addresses, dates of birth, Social Security numbers, driver's license and passport numbers, and financial positions and account numbers (transactional account numbers are generally truncated to the ending digits, though some investment and special purpose accounts may not be truncated).

Attribution 1 Publication: MD AG's office Author:
Article Title: Cultivian Ventures, LLC
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248649.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-07	Fairway Independent Mortgage Corporation	WI	1/23/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Maryland AG update: Our client Fairway Independent Mortgage Corporation ("Fairway") was the target of a cyber email attack. The emails that were accessed may have included personal information, such as name, social security number and/or financial information, of Maryland residents.

Attribution 1 Publication: MD AG's office Author:
Article Title: Fairway Independent Mortgage Corporation
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248648.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-06	Camp Bow Wow Franchising, Inc.	CO	1/23/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: After noticing a log-in issue with CBW's computers and conducting a prompt forensic investigation, CBW discovered on September 19, 2014 that its computer systems were compromised on September 7, 2014. Based on CBW's findings to date, CBW has leamed that an account with administrative-level access was compromised by an unknown third-party and used to reset all account passwords, which prevented authorized access for a limited period.

Attribution 1 Publication: MD AG's office Author:
Article Title: Camp Bow Wow Franchising, Inc.
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247196.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-05	Aarow Equipment & Services (Aarow Contracting, Inc.)	MD	1/23/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: On Oct 31, 2014, a company laptop was stolen from a vehicle. That laptop contained employees personal information such as: Name, Social Security Numbers, Birth Dates, Addresses, Driver's License Numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Aarow Equipment & Services (Aarow Contracting, Inc.)
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-246650.pdf

Attribution 2 Publication: Author:
Article Title:
Article URL:

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-04	Corday Productions, Inc. (Sony)	CA	1/23/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: We are writing to you because an entity (Sony Pictures Entertainment) that maintains personal infonnalion on behalf of Corday Productions, Inc. ("Corday") was recently the subject of a cyber attack during the last week of November. We understaod that the entity has not found evidence that the cyber attack has resulted in a sectrrity breach of the personal information pertaining to Corday's employees, independent contractors or employees of contractors providing services to Corday.

Attribution 1 Publication: MD AG's office Author:
Article Title: Corday Productions, Inc. (Sony)
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248473%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-03	Dutch Bros. Coffee	OR	1/23/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: On Saturday, December 6th, 2014, we received information that raised suspicion of an unauthorized breach of our website that was exposing the payment information for some customers of DutchWear. In order to best protect our customers, we immediately took down our e-commerce site shop.dutchbros.com and conducted an extensive investigation of our computer systems.

Attribution 1 Publication: MD AG's office Author:
Article Title: Dutch Bros. Coffee
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248477.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-02	API Group, Inc.	MN	1/23/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: On Monday morning, November 17, 2014, APi Group's home office sent an email to the employee benefits contact(s) at each of the APi Group companies asking them to follow-up with their employees who had not yet completed open enrollment for 2015. A couple of the email recipients then forwarded the email to employees at their company without deleting an attachment to the original email that contained the following personal information regarding APi Group companies' benefit eligible employees that is used for benefit enrollment purposes: first and last name, social security number, date of birth, tobacco user reporting, and medical and short-term disability plan enrollment status

Attribution 1 Publication: MD AG's office Author:
Article Title: API Group, Inc.
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247668.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150123-01	M&T Bank	NY	1/23/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Maryland AG update: It has recently come to our attention that due to an unfortunate matter involving the break-in of an employee vehicle, certain documents were stolen that may have included your personal information, such as your name, address, telephone number, social security number, and account numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: M&T Bank
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-246655.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-28	Wyndham Vacation Resorts	FL	1/22/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: Ten Wyndham timeshare owners from other states reported to Wyndham that there were unauthorized charges on their credit card account. Wyndham immediately commenced an investigation. Upon further investigation, Wyndham believes that between August 15, 2014, and September 22, 2014, a Wyndham employee, who previously assisted customers with the contract processing of their time share purchase, was possibly responsible for inappropriately using credit card information without authorization.

Attribution 1 Publication: MD AG's office Author:
Article Title: Wyndham Vacation Resorts
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247195.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-27	DLS Direct Learning Systems	PA	1/22/2015	Electronic	Business	Yes - Published #	1,507

Maryland AG update: On October 19, 2013 , an unauthorized party accessed our computer system and installed data that provided the attacker with continuing access to the system. We are not aware of any actions taken by the attacker utilizing that access until July 13, 2014, when the unauthorized third party attacker accessed our system to upload a phishing website that collected personal information of customers of a third party bank.

Attribution 1 Publication: MD AG's office Author:
Article Title: DLS Direct Learning Systems
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247185.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-26	Modern Gun School	PA	1/22/2015	Electronic	Business	Yes - Published #	287

Maryland AG update: On October 19, 2013, an unauthorized party accessed our computer system and installed data that provided the attacker with continuing access to the system. We are not aware of any actions taken by the attacker utilizing that access until July 13, 2014, when the unauthorized third party attacker accessed our system to upload a phishing website that collected personal information of customers of a third party bank.

Attribution 1 Publication: MD AG's office Author:
Article Title: Modern Gun School
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247182.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-25	c3controls	PA	1/22/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: On October 9, 2014, c3controls identified a potential breach of the security of our website. At this time, the information available to us is limited and our investigation of the situation is ongoing. However, based upon the information available to us at this time, it appears that information submitted by customers in placing orders by credit card through our website may have been compromised. We are contacting you because you placed a credit card order with the account number ending in #XXXX during the time period when we believe the breach occurred.

Attribution 1 Publication: MD AG's office Author:
Article Title: c3controls
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247018.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-24	Primerica	GA	1/22/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: Primerica has determined that a breach of personal information as defined in Md. Code Am1. §§ 14-3504 et seq. has occurred, and therefore, notification will be sent to parties who may be affected by the breach. On or about October 12, 2014, a laptop belonging to an independent contractor or representative of Primerica was stolen. The laptop was password protected, but it may have contained unencrypted imaged copies of life insurance docurnents containing personal information of four (4) Maryland residents.

Attribution 1 Publication: MD AG's office Author:
Article Title: Primerica
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247124.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-23	Pulte Mortgage LLC	CO	1/22/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Maryland AG update: On September 20, 2014, Pulte Mortgage became aware that a laptop belonging to one of our employees was stolen. While the laptop was encrypted, the password to the laptop may have accompanied the laptop and may have been available to the thief. The information contained on the laptop may have included names, addresses, phone or email, Social Security Numbers, or financial account numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Pulte Mortgage LLC
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248684.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-22	Waynesburg University	PA	1/22/2015	Electronic	Educational	Yes - Published #	284

Maryland AG update: I write to notify you of an incident at Waynesburg University (the "University") that resulted in the possible release of personal information of five (5) Maryland residents. On June 20, 2014, the University discovered that information for 284 students was saved to files on a drive that was capable of being accessed through the internet. The files in question contained names, addresses, telephone numbers, and in some instances, social security numbers of University students. Within hours of discovering the existence of the files, the University removed the files from the drive and disabled the internet link.

Attribution 1 Publication: MD AG's office Author:
Article Title: Waynesburg University
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-241980.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-21	McKenna Long & Aldridge	DC	1/22/2015	Electronic	Business	Yes - Published #	441

Maryland AG update: McKenna Long & Aldridge (“MLA”) recently learned of suspicious computer activity on servers belonging to one of our vendors, which stored information about MLA’s current and former employees. The vendor notified MLA of this suspicious activity on February 14, 2014 and MLA immediately began investigating this incident. As a result of that investigation and further information provided by the vendor, it appears that some information related to current and former employees was accessed on November 28, 2013, December 11, 2013, and December 12, 2013 and that such access was obtained through the malicious and unauthorized access to the user identification and password of an account administrator.

Attribution 1 Publication: MD AG's office Author:
Article Title: McKenna Long & Aldridge
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-237723.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-20	Blue Zebra Sports - American Athletic Conference	TN	1/22/2015	Electronic	Business	Yes - Published #	1,218

Maryland AG update: We are writing to notify you of unauthorized access to personal information involving 9 Maryland residents. The reason that we are providing this notice to you is that pproximately 1,218 total users were potentially impacted by this unauthorized access. We became aware of unauthorized access to officiating.com on October 9, 2014. After conducting an audit of our systems to determine the scope of the incident, we notified all our users on October 22, 2014. It appears from our audit that this unauthorized access occurred using administrative credentials illegally obtained by the users and only happened sporadically over the past three years.

Attribution 1 Publication: MD AG's office Author:
Article Title: Blue Zebra Sports
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248645.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-19	Worldwide Insurance Company (Experian)	AZ	1/22/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: This letter is to inform you that your personal information may have been accessed without proper authorization. This unauthorized access took place on 10/9/2014, Experian one of the nationwide credit reporting agencies, identified that its client, Worldwide Insurance Specialists, had certain Experian consumer information accessed without proper authorization. The consumer information consists of information typically found in a consumer report, Such information includes your name and address and one or more of the following: Social Security number, date of birth, or account numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Worldwide Insurance Company (Experian)
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247122.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-18	Sinclair Institute / Townsend Enterprises	NC	1/22/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: Our client initially learned of a potential breach on August 28, 2014 from its third party hosting company, on whose servers the breach occurred. The breach involved the modification of computer files without authorization (due to weak administrator credentials), which in turn allowed credit card information to be illegally captured. The compromised information includes: name and address of the consumer, user name and password for our website at www.sinclairinstitute.com, email address, birth date, phone number and payment card information (including card numbers, expiration dates and security codes).

Attribution 1 Publication: MD AG's office Author:
Article Title: Sinclair Institute / Townsend Enterprises
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247023.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-17	Metropolitan Life Insurance Company	NY	1/22/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: We write to inform you about an (incident or processing error) involving your personal information. Specifically, on insert Month, Day, Year [Briefly describe how incident occurred.]. We believe that the records contained sensitive personal information (e.g., your name, address, Social Security number, medical information).

Attribution 1 Publication: MD AG's office Author:
Article Title: Metropolitan Life Insurance Company
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-245146.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-16	Booking.com	CT	1/22/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: I am writing to inform you that Booking.com learned on or about September 2, 2014 that an external party accessed and used customers' personal information includ ing name,bill ing address, and credit card details. The suspicious activity appears to have taken place between approximately June 6, 2014 and September 15, 2014. T

Attribution 1 Publication: MD AG's office Author:
Article Title: Booking.com
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-245325%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-15	TREMEC	MI	1/22/2015	Electronic	Business	Yes - Unknown #	Unknown

We are bringing this to your attention as recently a TREMEC employee's vehicle was broken into resulting in the loss of a company issued computer as well as other personal belongings. We believe there may have been sensitive information contained on the hard drive.

Attribution 1 Publication: MD AG's office Author:
Article Title: TREMEC
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-245266.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-14	Nationstar Mortgage	TX	1/22/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Maryland AG update: We are writing to inform you of an incident involving personal information security breach. On August 5, 2014, a Nationstar Mortgage LLC employee inadvertently forwarded an e-mail to an outside company which contained borrowers' first and last names, addresses, and mortgage loan
numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Nationstar Mortgage
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-244309.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-13	Metropolitan State University	MN	1/16/2015	Electronic	Educational	Yes - Published #	160,000

Metropolitan State University has recently learned of a computer security intrusion and a likely data breach. We are investigating the scope of what appears to be unauthorized access to a university server that contained personal information of faculty, staff and students. We do not believe this server contained any financial data or credit card information, but several databases included employee Social Security Numbers.

Attribution 1 Publication: databreaches.net Author:
Article Title: Hacker breached Metropolitan State University database with personal info
Article URL: http://www.databreaches.net/category/breach-reports/us/page/2/

Attribution 2 Publication: databreaches.net Author:
Article Title: Metropolitan State University updates details on hack claimed by Abdilo
Article URL: http://www.databreaches.net/metropolitan-state-university-updates-details-on-hack-claimed-by-abdilo/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-12	Wingstop	TX	1/17/2015	Electronic	Business	Yes - Unknown #	Unknown

Wingstop today announced that four of its independently owned and operated franchise locations may have been impacted by a data security attack on point-of-sale (POS) systems that could have enabled attackers to capture customer payment card information such as account number, expiration date or cardholder name.

Attribution 1 Publication: databreaches.net Author:
Article Title: Wingstop Announces Data Security Incident Affecting Four Franchise Locations
Article URL: http://www.databreaches.net/category/breach-reports/us/page/2/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-11	University of Oregon	OR	1/21/2015	Electronic	Educational	Yes - Unknown #	Unknown

We have recently learned that a significant number of archived records from the President's Office have been unlawfully released. These records contain confidential information about faculty, staff and students, but our current understanding is that no social security numbers, financial information or medical records were shared.

Attribution 1 Publication: oregonlive.com Author:
Article Title: University of Oregon
Article URL: http://media.oregonlive.com/education_impact/other/an%20email.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-10	Merchant - American Express	AL	1/15/2015	Electronic	Business	Yes - Unknown #	Unknown

We are strongly committed to the security of our Cardmembers' information and strive to let you know about security concerns as soon as possible. A merchant where you used your American Express Card detected unauthorized access to their website files. At this time, we believe the merchant's affected data files included your American Express Card account number, your name and other Card information such as the expiration date. Importantly, your Social Security number was not impacted and our systems have not detected any unauthorized activity on your Card account related to this incident.

Attribution 1 Publication: CA AG's office Author:
Article Title: Merchant - American Express
Article URL: https://oag.ca.gov/system/files/CA%20AG_Customer%20Letter%20-%20C2014070234_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-09	Oppenheimer Funds	CO	1/15/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On January 9, 2015, a brokerage firm ("Firm") that has a business relationship with us notified us that, on April 24, 2014, your name, address, Oppenheimer Fund account number, and social security number were erroneously made accessible to a registered representative of the Firm.

Attribution 1 Publication: CA AG's office Author:
Article Title: Oppenheimer Funds
Article URL: https://oag.ca.gov/system/files/CA%20Security%20Breach%20Notification%20Sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-08	American Airlines	TX	1/7/2015	Electronic	Business	Yes - Unknown #	Unknown

We are writing to inform you about an incident involving unauthorized access to your online AAdvantage* accounl An unauthorized third party recently used email addresses and passwords obtained from sources other than American Airlines to log into certain accounts, including yours. This could have resulted in access to the information that you see when you log in to your account, such as your name, email address, phone number, postal address, date of birth, the last four digits of your credit or debit card and its expiration date, your AAdvantage number, and information about the miles, mileage activity, the points that you have accrued, and the last four digits of passport numbers.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-07	United Airlines	IL	1/22/2015	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that an unauthorized party attempted to access your MileagePius® account with usernames and passwords obtained from a third-party source. These usernames and passwords were not obtained as a result of a United® data breach, and United was not the only company where attempts were made.

Attribution 1 Publication: CA AG's office Author:
Article Title: United Airlines
Article URL: https://oag.ca.gov/system/files/CA%20Notification1_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-06	Law Offices of David A. Krausz, P.C.	CA	1/12/2015	Electronic	Business	Yes - Unknown #	Unknown

On January 6, 2015, Law Offices of David A. Krausz, P.C. experienced the theft of a laptop computer that contained identifying client information including names, social security numbers and dates of birth. As a result of this incident, information identifiable with you was potentially exposed to others. The theft was reported to the San Francisco Police Department and a report was filed.

Attribution 1 Publication: CA AG's office Author:
Article Title: Law Offices of David A. Krausz, P.C.
Article URL: https://oag.ca.gov/system/files/Security%20Breach%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-05	ValuePetSupplies.com / Piech Sales Company	TN	1/12/2015	Electronic	Business	Yes - Unknown #	Unknown

Piech Sales Company, LLC d/b/a ValuePetSupplies.com is contacting you about an incident regarding a breach of our computer system that involves your personal information. On or about November 25, 2014, ValuePetSupplies.com was the victim of a cyberattack. Unauthorized persons accessed our servers and installed malicious files to capture personal information entered by individuals onto our website (http://www.valuepetsupplies.com)

Attribution 1 Publication: CA AG's office / scmagazine.com / NH Author:
Article Title: ValuePetSupplies.com / Piech Sales Company
Article URL: https://oag.ca.gov/system/files/Sample%20Breach%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-04	**Barbecue Renew / Grillparts.com**	FL	1/22/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Barbecue Renew, Inc., (“Barbecue Renew” or “us” or “we”), is an e-commerce retailer offering grill accessories, equipment and replacement parts through our website www.grillparts.com. You are receiving this notification because at some point in the past, you completed a purchase through our website which required you to provide us with your credit card information. We have determined that your cardholder data, which may include your first and last name, address, personal card account number, expiration date, and card security codes, may have been compromised as a result of a series of cyber attacks on our web server

Attribution 1 Publication: CA AG's office / esecurityplanet.com Author:
Article Title: Barbecue Renew / Grillparts.com
Article URL: https://oag.ca.gov/system/files/Barbecue%20Renew%20Consumer%20Notification%20Sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-03	**Six Red Marbles, LLC**	MA	1/15/2015	Electronic	Business	Yes - Unknown #	**Unknown**

We recently learned of a potential breach involving your personal information. Specifically, certain 1099 tax information that Six Red Marbles, LLC had provided to an independent outside vendor for processing had been placed by that vendor on an unprotected FTP site. The data placed on the FTP site included names, addresses, dates of birth and social security numbers, and may have been on the FTP server since September 2014.

Attribution 1 Publication: VT AG's office Author:
Article Title: Six Red Marbles, LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Six%20Red%20Marbles%20Security%20Breach%20Not

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-02	**St. Louis County's Department of Health**	MO	1/15/2015	Electronic	Government/Military	Yes - Published #	**4,000**

St. Louis County has learned that some personal information belonging to inmates was handled inappropriately at the St. Louis County’s Buzz Westfall Justice Center. Specifically, on November 18, 2014, it was discovered that a health department employee had e-mailed a document containing the names and social security numbers of inmates incarcerated from 2008 to 2014 to a personal e-mail account belonging to that same employee. Although no one other than that county employee is known to have had access to the information in that document, the action still constitutes a breach of federal law – specifically, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). [County Department of Health]

Attribution 1 Publication: phiprivacy.net / stlouisco.com / hhs.gov Author:
Article Title: St. Louis County Dept. of Health investigates HIPAA breach involving inmates
Article URL: http://www.phiprivacy.net/st-louis-county-dept-of-health-investigates-hipaa-breach-involving-inmates/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150122-01	**Sunglo Home Health Services**	TX	1/22/2015	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

Sunglo Home Health Services has thousands of patients across the Valley. Their personal information is in the hands of a Harlingen burglar. He walked away with sensitive information and it was all caught on surveillance video.

Attribution 1 Publication: krgv.com Author:
Article Title: Computer with Patients’ Personal Information Stolen
Article URL: http://www.krgv.com/news/local-news/Computer-with-Patients-Personal-Information-Stolen/30850638

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150121-09	Rentrak Corporation	OR	1/21/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: I am writing on behalf of Rentrak Corporation to inform you of a recent security breach incident involving the theft of password-protected computer equipment from the car of a human resources employee. The theft occurred Friday, September 12, and was discovered shortly thereafter. In violation of several Rentrak data security policies, the laptop contained files containing name, address, social security number, and title and salary information for current Rentrak employees, including 1 resident of your state.

Attribution 1 Publication: MD AG's office Author:
Article Title: Rentrak Corporation
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-245331.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150121-07	Columbia Southern University	AL	1/21/2015	Electronic	Educational	Yes - Unknown #	Unknown

Maryland AG update: We represent Columbia Southern University (“CSU”), with respect to a recent security incident involving the potential exposure of certain personally identifiable information described in more detail below. CSU provided notification of this event to these individuals and is providing you with this letter in compliance with state notification requirements. CSU is a private university based in Orange Beach, Alabama, providing higher education to its students through online degree programs at the associate, bachelor and master degree levels. CSU takes the security of the information in its control very seriously.

Attribution 1 Publication: MD AG's office Author:
Article Title: Columbia Southern University
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247025.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150121-06	City of Alexandria, VA / Fire Department / ADP	VA	1/21/2015	Electronic	Government/Military	Yes - Unknown #	Unknown

Maryland AG update: On behalf of Advanced Data Processing, Inc. and its subsidiaries (the "Company") and the City of Alexandria, Virginia, and the City of Alexandria Fire Department (collectively, the "Agency") we are writing to provide you notice concerning the personal information of certain residents of your state. In the case of the Agency this is an initial notice, and in the case of the Company this notice supplements a prior notice provided to your office, concerning the incident covered by this notice.

Attribution 1 Publication: MD AG's office Author:
Article Title: City of Alexandria, VA / Fire Department / ADP
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247217.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150121-05	Polish Falcons of America	PA	1/21/2015	Electronic	Business	Yes - Unknown #	Unknown

Maryland AG update: I am writing to you on behalf of my client the Polish Falcons of America ("Polish Falcons"), a Pennsylvania nonprofit fraternal benefit society organization. The Polish Falcons are providing notice pursuant to Md. Code Ann. Comm. Law § 14-3 5 04 of a data security incident in which an unknown individual or individuals broke into their national headquarters and stole laptop and desktop computers. The computers contained personal information of both non-Members and Members of the Polish Falcons, including Social Security numbers and five credit card numbers.Based on its investigation, the Polish Falcons will notify one (1) Maryland resident on August 6, 2014.

Attribution 1 Publication: MD AG's office Author:
Article Title: Polish Falcons of America
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-244326.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150121-04	**Azusa Pacific University**	CA	1/21/2015	Electronic	Educational	Yes - Unknown #	**Unknown**

Maryland AG update: Our client Azusa Pacific University ("University") is writing to inform you of an incident involving the theft of a laptop computer that may have contained the name and social security number of two (2) Maryland residents.
During the night on November 17, 2014, a password protected laptop computer was stolen from the backseat of an employee's locked vehicle. The employee discovered the theft the following morning and immediately notified the University and the City of Orange Police Department. Immediately after learning of the theft, the University activated special security software designed to remotely delete all data on the laptop the next time it was turned on and connected to the Internet. We received confirmation that the data was deleted on November 21, 2014.

Attribution 1 Publication: MD AG's office Author:
Article Title: Azusa Pacific University
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-248474.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150121-03	**Allied-Barton**	PA	1/21/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Maryland AG update: We are writing to inform you regarding a security incident involving your information. As you know, AlliedBarton takes the privacy and security of employee and job applicant information very seriously. We are writing you because we recently became aware that certain personal information regarding a limited number of individuals who applied to be considered for a position within the company may have been electronically sent by one employee to another employee who was unauthorized to have access to that information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Allied-Barton
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247680.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150121-02	**PineBridge Investments / Benefit Express Services**	IL	1/21/2015	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

Maryland AG update: We represent Benefit Express Services (“BES”), with respect to a recent security incident involving the potential exposure of certain personally identifiable information described in more detail below. BES provided notification of this event to these individuals and is providing you with this letter in compliance with state notification requirements. BES takes the security of the information in its control very seriously. Accordingly, it has identified individuals whose personally identifiable information may have been exposed in the incident discussed below, and provided appropriate services to them including monitoring and identity theft restoration. (Maryland = 379)

Attribution 1 Publication: MD AG's office Author:
Article Title: Benefit Express Services
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247019.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150121-01	**Asset Marketing Services / GovMint.com**	MN	1/21/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Maryland AG update: Please accept this letter on behalf of Asset Marketing Services, LLC (d/b/a GovMint.com) ("AMS") as notification under the Maryland Personal Information Protection Act of a security incident that occurred between September 18, 2014 and October 2, 2014. The incident involved unauthorized changes made to our website, www.govmint.com, which resulted in unaut horized access to personal information of 30 Maryland residents, during the web ordering process

Attribution 1 Publication: MD AG's office Author:
Article Title: Asset Marketing Services / GovMint.com
Article URL: http://www.oag.state.md.us/idtheft/Breach%20Notices/itu-247037.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150114-02	**Inland Empire Health Plan (IEHP) / Children's Eyewear**	CA	1/9/2015	Electronic	Medical/Healthcare	Yes - Published #	**1,030**

Inland Empire Health Plan (IEHP) is notifying plan members of a breach at a local provider's facility. On October 28, a desktop computer and other items were reportedly stolen from Children's Eyewear Sight in Rancho Cucamonga, CA. A file on the computer included plan members' name, date of birth, gender, address and contact phone number, email address, IEHP Member ID number, appointment date, date of purchase, and the name of the doctor who provided the optical prescription. Some of those affected were plan members' dependent children.

Attribution 1 Publication: phiprivacy.net / CA AG's office Author:
Article Title: Inland Empire Health Plan notifies Children's Eyewear Sight customers of data theft (Update1)
Article URL: http://www.phiprivacy.net/inland-empire-health-plan-notifies-childrens-eyewear-sight-customers-of-data-theft/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150109-01	**Libbey Inc.**	OH	1/8/2015	Electronic	Business	Yes - Unknown #	**Unknown**

Libbey Inc. understands the importance of protecting personal information. We are writing to inform you about a recent incident involving your information.
In connection with our efforts to comply with the Foreign Account Tax Compliance Act, our credit department created a spreadsheet identifying the distributor sales representatives who receive spiff payments from Libbey, but from whom Libbey had not yet received the required W-8 or W-9 form. The spreadsheet listed your name, address, and Social Security number.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Libbey Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Libbey%20Inc%20Letter%20to%20Consumer%20Secur

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150107-03	**Art of Tea**	CA	1/5/2015	Electronic	Business	Yes - Unknown #	**Unknown**

We are writing to notify you of a data security incident that may have involved your payment card data from purchases that you made at on our website. Art of Tea is committed to protecting your data and regrets any inconvenience caused by this incident. We apologize for the frustration and anxiety this causes our customers and as set forth below.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150107-02	**Aspire Indiana, Inc.**	IN	1/6/2015	Electronic	Medical/Healthcare	Yes - Published #	**43,890**

We are writing to inform you of an incident at Aspire Indiana, Inc. ("Aspire") (formerly known as The Center for Mental Health or BehaviorCorp.) that may have resulted in the disclosure of your personal information, including your name and limited personal health information. Your Social Security number and electronic medical health records were not exposed, and remain secure. Number of records per HHS.gov

Attribution 1 Publication: phiprivacy.net / hhs.gov Author:
Article Title: Aspire Indiana notifies over 45,000 employees and clients after burglars nab office laptops
Article URL: http://www.phiprivacy.net/aspire-indiana-notifies-over-45000-employees-and-clients-after-burglars-nab-office-laptops/

Attribution 2 Publication: VT AG's office / phiprivacy.net Author:
Article Title: Aspire Indiana, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Aspire%20SBN%20to%20Consumer.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150107-01	**Fast Forward Academy**	FL	1/7/2015	Electronic	Business	Yes - Unknown #	**Unknown**

We were recently notified that an unauthorized person attempted to access our systems. These systems store customer information such as names, addresses, payment account numbers, and/or email addresses.

Attribution 1 Publication: CA AG's office Author:
Article Title: Fast Forward Academy
Article URL: https://oag.ca.gov/system/files/Notification%20Letter%20Fast%20Forward%20Academy_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150105-02	La Jolla Group	CA	1/2/2015	Electronic	Business	Yes - Unknown #	Unknown

La Jolla Group, a management company that provides management services in connection with the operation of ecommerce websites to certain apparel brand licensees, is writing to notify you of a data security incident that affects the security·of your personal information, and to make you aware of resources available to support you.

Attribution 1 Publication: CA AG's office Author:
Article Title: La Jolla Group
Article URL: https://oag.ca.gov/system/files/CA%20Exhibit%20A%20revised_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20150105-01	Morgan Stanley	NY	1/5/2015	Electronic	Banking/Credit/Financial	Yes - Published #	350,000

Morgan Stanley fired an employee it said stole data, including account numbers, for as many as 350,000 wealth-management clients and posted some of the information online. The bank alerted law enforcement and found no evidence that customers lost any money, New York-based Morgan Stanley said today in a statement. The firm said it detected account information for about 900 clients on an external website and “promptly” had it removed. 350,000 records accessed however only 900 appeared online.

Attribution 1 Publication: bloomberg.com Author: Michael J. Moore
Article Title: Morgan Stanley
Article URL: http://www.bloomberg.com/news/print/2015-01-05/morgan-stanley-fires-employee-accused-of-stealing-client-data.html

Attribution 2 Publication: zdnet.com Author: Charlie Osborne
Article Title: Morgan Stanley sacks employee who pilfered account data
Article URL: http://www.zdnet.com/article/morgan-stanley-sacks-employee-who-pilfered-account-data/

2015 Breaches Identified by the ITRC as of:	12/29/2015

Total Breaches:	780
Records Exposed:	177,866,236

The ITRC Breach database is updated on a daily basis, and published to our website on Tuesday. Unless noted otherwise, each report includes breaches that occurred in the year of the report name (such as "2014 Breach List"), or became public in the report name year, but were not public in the previous year. Each item must be previously published by a credible source, such as an Attorney General's website, network television, national print media, etc. The item will not be included if the ITRC is not certain that the source is real and credible. We include, for each incident, a link or source of the article, and the information presented by that article. Many times, we have attributions from a multitude of media sources and media outlets. ITRC sticks to the facts as reported, and does not add or subtract from the previously published information. When the number of exposed records is not reported, we note that fact. Note: For data breach incidents involving only emails, user names, and/or passwords, the number of records are not included in the overall total number of records.

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

The ITRC Breach Report presents individual information about data exposure events and running totals for the year.

The ITRC Breach Stats Report develops some statistics based upon the type of entity involved in the data exposure.

The ITRC would like to thank IDentityTheft911 for its financial support of the ITRC Breach Report, ITRC Breach Stats Report and all supplemental breach reports.