ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-99	**Honeyville Grain Online**	UT	7/31/2017	Electronic	Business	Yes - Published #	**321**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Honeyville Grain Online
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-98	**Holabird Sports**	MD	7/1/2017	Electronic	Business	Yes - Published #	**Unknown**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Holabird Sports
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-97	**HK Parts**	UT	7/1/2017	Electronic	Business	Yes - Published #	**910**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: HK Parts
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-96	**HDIS**	MO	7/1/2017	Electronic	Business	Yes - Published #	**15,422**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: HDIS
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-95	**Hard Rock Hotel & Casino**	NV	7/1/2017	Electronic	Business	Yes - Published #	**486**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Hard Rock Hotel & Casino
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-94	**Fun Eats and Drinks**	OH	7/1/2017	Electronic	Business	Yes - Published #	**5,730**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Fun Eats and Drinks
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-93	FatQuarterShop.com	TX	7/1/2017	Electronic	Business	Yes - Published #	601

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: FatQuarterShop.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-92	Evereve #99	MN	7/1/2017	Electronic	Business	Yes - Published #	1,989

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Evereve #99
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-91	Essick Air Products	AR	7/1/2017	Electronic	Business	Yes - Published #	1,355

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Essick Air Products
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-90	Dumac Business Systems, Inc.	PA	7/1/2017	Electronic	Business	Yes - Published #	61,070

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office (per notification from Dis Author:
Article Title: Dumac Business Systems, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-89	CZ Custom 2	AZ	7/1/2017	Electronic	Business	Yes - Published #	129

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: CZ Custom 2
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-88	Clark County	NV	7/1/2017	Electronic	Government/Military	Yes - Published #	1,430

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Clark County
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-87	Brilliant Book House	WA	7/1/2017	Electronic	Business	Yes - Published #	167

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Brilliant Book House
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-86	Blue Chip Athletic Inc.	MO	7/1/2017	Electronic	Business	Yes - Published #	150

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Blue Chip Athletic Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-85	Barista Pro Shop	CO	7/1/2017	Electronic	Business	Yes - Published #	108

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Barista Pro Shop
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-84	Dattner Architects	NY	7/1/2017	Electronic	Business	Yes - Published #	125

Per Notification NY AG's office
Description of Breach: unclear if it was internal system or third party system (payroll company, etc)
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Dattner Architects
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-83	CSM Bakery Solutions	GA	7/1/2017	Electronic	Business	Yes - Published #	949

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

Attribution 1 Publication: NY AG's office Author:
Article Title: CSM Bakery Solutions
Article URL: Per FOIL NY AG's Office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-82	Crane, Tonelli, Rosenberg & Co., LLP	PA	7/1/2017	Electronic	Business	Yes - Published #	463

Per Notification NY AG's office
Description of Breach: External systems breach
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Crane, Tonelli, Rosenberg & Co., LLP
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-81	Canali Trading LLC	NY	7/1/2017	Electronic	Business	Yes - Published #	133

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Canali Trading LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-80	CPA Tax Planning	NY	7/1/2017	Electronic	Business	Yes - Published #	603

Per Notification NY AG's office
Description of Breach: Hackers attempting to gain access to clients' tax information for the purpose of filing fraudulent returns.
Information Acquired: SSN

Attribution 1 Publication: NY AG's Office Author:
Article Title: CPA Tax Planning
Article URL: Per FOIL NY AG's Office

Attribution 2 Publication: NY AG's office Author:
Article Title: CPA Tax Planning
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-79	Atlantic Firearms	MD	7/1/2017	Electronic	Business	Yes - Published #	224

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Atlantic Firearms
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-78	American Association Notaries	TX	7/1/2017	Electronic	Business	Yes - Published #	326

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: American Association Notaries
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-77	www.atbatt.com	CA	8/11/2017	Electronic	Business	Yes - Published #	165

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: www.atbatt.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-76	WAY.COM (10/2017)	CA	10/10/2017	Electronic	Business	Yes - Published #	6,854

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: WAY.COM (10/2017)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-75	URBANOG.COM	CA	7/12/2017	Electronic	Business	Yes - Published #	295

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: URBANOG.COM
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-74	Beauty Place (The)	FL	9/7/2017	Electronic	Business	Yes - Published #	161

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Beauty Place (The)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-73	Saladworks	NJ	7/12/2017	Electronic	Business	Yes - Published #	224

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Saladworks
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-72	Rebecca Minkoff, LLC	NY	7/12/2017	Electronic	Business	Yes - Published #	4,485

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Rebecca Minkoff, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-71	Magills GV Glockstore	CA	9/7/2017	Electronic	Business	Yes - Published #	2,486

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Magills GV Glockstore
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-70	Insect Lore	CA	9/7/2017	Electronic	Business	Yes - Published #	315

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Insect Lore
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-69	INET, Inc.	DC	7/20/2017	Electronic	Business	Yes - Published #	775

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: INET, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-68	Framesbymail	MO	9/7/2017	Electronic	Business	Yes - Published #	307

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Framesbymail
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-67	Double R Restaurant	FL	7/12/2017	Electronic	Business	Yes - Published #	110

Per FOIL NY AG's office.

Attribution 1 Publication: Author:
Article Title: Per FOIL NY AG's office (per notification from Discover)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-66	Designoptics.com	NY	7/12/2017	Electronic	Business	Yes - Published #	100

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office. Author:
Article Title: Designoptics.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-65	Commercial Industrial Supply	SC	9/7/2017	Electronic	Business	Yes - Published #	300

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Commercial Industrial Supply
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-64	**Cable Ties and More**	WY	7/12/2017	Electronic	Business	Yes - Published #	**131**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Cable Ties and More
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-63	**Buffalo Jackson Trading Co., LLC**	NC	9/7/2017	Electronic	Business	Yes - Published #	**273**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Buffalo Jackson Trading Co., LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-62	**Bizignition Technologies**	US	7/12/2017	Electronic	Business	Yes - Published #	**175**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Bizignition Technologies
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-61	**American Tombow, Inc.**	GA	9/7/2017	Electronic	Business	Yes - Published #	**105**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: American Tombow, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-60	**Sweetgreen LLC**	NY	7/13/2017	Electronic	Business	Yes - Published #	**104**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Sweetgreen LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-59	**Academy of Model Aeronautics**	IN	7/1/2017	Electronic	Business	Yes - Published #	**5,428**

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Academy of Model Aeronautics
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-58	Congressional Hispanic Caucus Institute	DC	7/1/2017	Electronic	Business	Yes - Published #	133

Per Notification NY AG's office
Description of Breach: Insider wrongdoing
Information Acquired: SSN and driver's license

Attribution 1 Publication: NY AG's office Author:
Article Title: Congressional Hispanic Caucus Institute
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-57	Codman Square Health Center	MA	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	357

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Codman Square Health Center
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-56	Clutch Analytics, LLC	TX	7/1/2017	Electronic	Business	Yes - Published #	4,225

Per Notification NY AG's office
Description of Breach: External systems breach / Virus (including 'Trojan Horse', 'Phishing' or other use of malicious code)
Other Description: Ransomware
Information Acquired: Driver's license

Attribution 1 Publication: Per FOIL NY AG's office Author:
Article Title: Clutch Analytics, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-55	Cleveland Metropolitan School District	OH	7/1/2017	Electronic	Educational	Yes - Published #	1,307

Per Notification NY AG's office
Description of Breach: Hacking/phishing
Information Acquired: SSN and Driver's License

Attribution 1 Publication: NY AG's office Author:
Article Title: Cleveland Metropolitan School District
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-54	Clarke University	IA	7/1/2017	Electronic	Educational	Yes - Published #	443

On February 7, 2017, Clarke University learned that one of its employees received a phishing email designed to appear as if it came from another employee. Although the investigation is ongoing, Clarke University determined that the unauthorized individual may have accessed some of its employees IRS Form W-2s for tax year 2016, which included names, addresses, and Social Security numbers.

Attribution 1 Publication: NY AG's office Author:
Article Title: Clarke University
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-53	Capital Insurance Group	CA	7/1/2017	Electronic	Business	Yes - Published #	557

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Capital Insurance Group
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-52	Chartwell Hospitality LLC	TN	7/1/2017	Electronic	Business	Yes - Published #	1,636

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Chartwell Hospitality LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-51	Cornell University (3/17)	NY	7/1/2017	Electronic	Educational	Yes - Published #	103

Per Notification NY AG's office
Description of Breach: Misuse of stolen university credentials
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Cornell University (3/17)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-50	Coley, Eubank & Company, PC	VA	7/1/2017	Electronic	Business	Yes - Published #	753

Per Notification NY AG's office
Description of Breach: External system breach (e.g. hacking)
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Coley, Eubank & Company, PC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-49	Citibank, NA (2/17)	NY	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	164

Per Notification NY AG's office
Description of Breach: A former employee believed to have facilitated unauthorized access to data
Information Acquired: Undefined

Attribution 1 Publication: NY AG's office Author:
Article Title: Citibank, NA
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-48	SEKO Worldwide, LLC	IL	7/1/2017	Electronic	Business	Yes - Published #	256

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

Attribution 1 Publication: NY AG's office Author:
Article Title: SEKO Worldwide, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-47	Cornell University (2/17)	NY	7/1/2017	Electronic	Educational	Yes - Published #	308

Per Notification NY AG's office
Description of Breach: External system breach (e.g. hacking)
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Cornell University
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-46	SMH Enterprises LLC	LA	7/1/2017	Electronic	Business	Yes - Published #	14,196

Per Notification NY AG's office
Description of Breach: external system breach (e.g. hacking)
Information Acquired: Undefined

Attribution 1 Publication: Author:
Article Title: SMH Enterprises LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-45	Brown Brothers Harriman & Co.	NY	7/1/2017	Electronic	Business	Yes - Published #	249

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Brown Brothers Harriman & Co.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-44	Arrhythmia Institute dba Mercer Bucks Cardiology	PA	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	189

Per Notification NY AG's office
Description of Breach: Insider wrongdoing
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Arrhythmia Institute dba Mercer Bucks Cardiology
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-43	Nussbaum Yates Berg Klein & Wolpow, LLP	NY	7/1/2017	Electronic	Business	Yes - Published #	134

Recently, we learned that documents stored on our vendor's secure online document storage portal had been accessed by an unknown and unauthorized party. Due to the nature of financial documents maintained on the document storage portal, the documents that were accessed without authorization contained the names, social security numbers, drivers' license numbers and/or financial account numbers of our clients, their family members and/or their employees

Attribution 1 Publication: NY AG's office Author:
Article Title: Nussbaum Yates Berg Klein & Wolpow, LLP
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-42	A&M LLC	NY	7/1/2017	Electronic	Business	Yes - Published #	3,356

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: A&M LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-41	24 x 7	TX	7/1/2017	Electronic	Business	Yes - Published #	2,009

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: 24 x 7
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-40	CBEW Professional Group, LLP	OK	7/1/2017	Electronic	Business	Yes - Published #	3,614

On May 26, 2017, we received a report from our forensic investigation confirming that we were the victim of a cyber-attack by which an unknown third party was able to access our computer network and some of our clients' personal information. As a result, some of your personaJ information may have been exposed to others, including your first and last name, home address, social security number, and 2015 and 2016 tax return information, including compensation data.

Attribution 1 Publication: NY AG's office Author:
Article Title: CBEW Professional Group, LLP
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-39	Baublebar, Inc.	NY	7/1/2017	Electronic	Business	Yes - Published #	231

We recently discovered that this year there was a misdirected communication, which compromised select employment records of Bauble Bar, Inc.

Attribution 1 Publication: NY AG's office Author:
Article Title: Baublebar, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-38	Bed Bath & Beyond	NJ	7/1/2017	Electronic	Business	Yes - Published #	101

It has come to our attention that one of our store employees processing an online order illegally compromised one of our other customer's credit card Information at our Bed Beth & Beyond store located at 550 E. Lancaster Avenue in Radnor, PA.

Attribution 1 Publication: NY AG's office Author:
Article Title: Bed Bath & Beyond
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-37	ANRO Inc.	PA	7/1/2017	Electronic	Business	Yes - Published #	149

Per Notification NY AG's office
Description of Breach: The incident involves an email spoofing attack.
Information Acquired: W-2 information with SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: ANRO Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-36	Shift Acupuncture	CA	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	237

On January 12, 2017, I learned that my office building was broken into the night before, and along with other individual offices, Shift Acupuncture Collective was burglarized. Relevantly, one password protected laptop was stolen from my office. The system contained: patients' first and last names, their email address, telephone number, appointment day and time, type of appointment (i.e., private acupuncture, group acupuncture, cupping, etc.) and cost.

Attribution 1 Publication: NY AG's office Author:
Article Title: Shift Acupuncture
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-35	Ameriprise Financial (6/17)	MN	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	254

Per Notification: Franchise advisor uploaded a client list containing PII to unsecure personal email account. Social Security number was exposed.

Attribution 1 Publication: NY AG's office Author:
Article Title: Ameriprise (6/17)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-34	Ameriprise (5/17)	MN	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	180

On April 11, 2017 I sent an unencrypted list of Eden Brewery Inc. employees using my personal email account, to an employee of Lhe brewery. That list included your name, date of birth and Social Security Number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Ameriprise (5/17)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-33	Ameriprise Financial (1/17)	MN	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	372

Per Notification NY AG's office
Description of breach: inadvertent exposure
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Ameriprise Financial (1/17)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-32	Netlink Software Group America, Inc.	MI	7/14/2017	Electronic	Business	Yes - Unknown #	Unknown

As you have already been informed, we recently fell victim to a social engineering scam on July 7, 2017, which resulted in the disclosure of your W-2 information. This information includes name, address, social security number and salary data.

Attribution 1 Publication: NY AG's office Author:
Article Title: Netlink Software Group America, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-31	Navy Federal Credit Union	VA	10/11/2017	Electronic	Banking/Credit/Financial	Yes - Published #	205

This incident was not part of a cyber attack on Navy Federal systems, but rather it was related to an individual's criminal activity.We are writing to notify you of an incident involving unauthorized access to your personal and financial information.

Attribution 1 Publication: NY AG's office Author:
Article Title: Navy Federal Credit Union
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-30	Mr. Cooper (9/27/2017)	TX	9/27/2017	Electronic	Banking/Credit/Financial	Yes - Published #	233

On or about June 16, 2017, an incident occurred where your loan number, property address and co-borrowers name (if applicable) were inadvertently populated on another borrowers letter. This resulted in another borrower seeing your loan number, property address and co-borrowers name (if applicable).

Attribution 1 Publication: NY AG's office Author:
Article Title: Mr. Cooper
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-29	Moog Inc.	NY	8/22/2017	Electronic	Business	Yes - Published #	247

For a brief time yesterday two emails were circulated internally within Moog by a Moog privileged user containing your Personally Identifiable Information (PII), specifically, your name, driver's license number and date of birth. Though the purpose was to update records for a legitimate business purpose, the cross-sharing of employee PII is not allowed except between appropriate privileged users (eg., HR, Risk Management, etc.) employee supervisors and their reporting employees.

Attribution 1 Publication: NY AG's office Author:
Article Title: Moog Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-28	MediaMath IT and HR	NY	8/16/2017	Electronic	Business	Yes - Unknown #	Unknown

As confirmation of your conversations with MediaMath IT and HR, MediaMath was recently targeted in a phishing scam. These documents may include your name, address, Social Security Number, income, and othersensitive data.

Attribution 1 Publication: NY AG's office Author:
Article Title: MediaMath IT and HR
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-27	Michael Saunders & Company	FL	8/25/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 6, 2017, Michael Saunders learned that several employees had received phishing emails requesting recipients to surrender the credentials to their email accounts.The investigation has determined your personal information may have been accessible in the compromised email account because it was contained on a W9 form submitted Michael Saunders for your work as an agent.

Attribution 1 Publication: NY AG's office / NH AG's office Author:
Article Title: Michael Saunders & Company
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-26	MA Higher Education Assistance Corp. dba	MA	7/1/2017	Electronic	Business	Yes - Published #	323

On April 19, 2017 ASA was notified by our Collection Agency that a report containing your personal information was inadvertently provided to their third-party auditor. The contents of the report included your name, address, phone number, and social security number.

Attribution 1 Publication: NY AG's office Author:
Article Title: MA Higher Education Assistance Corp. dba American Student Assistance
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-25	Merchant e-Solutions	GA	9/26/2017	Electronic	Business	Yes - Published #	496

On May 19, 2017, a Merchant e-Solutions employee detennined that one of the programs associated with our Business Platform system could be used to access certain documents from the Internet without first requiring valid login credentials. More specifically, the documents were related to merchant applications for card processing services and may have included your name, address, social security number, driver's license or other government identification number, or bank account number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Merchant e-Solutions
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-24	Legacy Consulting Group, LLC	KY	8/10/2017	Electronic	Business	Yes - Published #	2,164

Specifically, on June 26, 2017, Legacy discovered that legitimate remote log-on credentials had been unlawfully used by an unknown actor to gain improper access to its computer system. The security incident has been classified as a data breach due to the type of information accessed during the incident, which included individual's full names, social security numbers, addresses, financial information, children's names, dates of birth, and other information relevant and necessarily provided in preparing and filing tax forms with the Internal Revenue Service.

Attribution 1 Publication: NY AG's office Author:
Article Title: Legacy Consulting Group, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-23	LendFi	NY	8/10/2017	Electronic	Banking/Credit/Financial	Yes - Published #	800

Per Notification NY AG's office
Description of breach: Insider wrongdoing
Information acquired in combination with name or other personal identifiers: Personal information (date of birth, etc.); financial information (account number or credit/debit card number, in combination with the security code, password, or PIN for the account; Social Security number; Password/account information; Driver's license number (or non-driver identification card number.

Attribution 1 Publication: NY AG's office Author:
Article Title: LendFi
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-22	Law Office of Arthur Heitzer	WI	9/28/2017	Electronic	Business	Yes - Published #	538

On or about May 16, 2017, we discovered that our firm's external hard drive was missing. The information contained on the missing hard drive included information you provided to us, or which was supplied to us, in connection with any legal services that were rendered to you by our firm, which included your full name, date of birth and Social Security number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Law Office of Arthur Heitzer
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-21	Lanier, Westerfield, Deal & Proctor, CPAs	GA	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 7, 2017, we discovered a mailing error may have caused your 1099 form to have been inadvertently sent to another 1099 recipient. The 1099 form contained personal information about you, including your name, address, Social Security number, and income information.

Attribution 1 Publication: NY AG's office Author:
Article Title: Lanier, Westerfield, Deal & Proctor, CPAs
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-20	Kemmerer & Schooley, PLLC	VA	9/26/2017	Electronic	Business	Yes - Published #	420

On May 23, 2017, I received an email that appeared to be from someone I knew. The email contained an attachment, which I opened. This information could include social security numbers, bank account numbers, or credit Card information.

Attribution 1 Publication: NY AG's office Author:
Article Title: Kemmerer & Schooley, PLLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-19	Jeffrey Glasser, CPA, LLC	NY	7/21/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 23, 2017, I discovered that an unknown, unauthorized third-party may have accessed your personal information within my email account. The potentially compromised information includes your name, Social Security number and tax information.

Attribution 1 Publication: NY AG's office Author:
Article Title: Jeffrey Glasser, CPA, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-18	McMahon Agency	NY	10/10/2017	Electronic	Business	Yes - Published #	435

On September 27, 2017, the McMahon Agency discovered that personal information of two clients was inadvertently emailed to an unintended recipient. The investigation determined that the clients' names, addresses, phone numbers, insurance policy numbers and bank account information were inadvertently disclosed.

Attribution 1 Publication: NY AG's office Author:
Article Title: McMahon Agency
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-17	**Jaffa Simmons PLLC**	AZ	8/25/2017	Electronic	Business	Yes - Published #	**482**

On July 11, 2017, Jaffa Simmons computer systems were affected by ransomware that encrypted files and rendered them temporarily unavailable. At the time of this incident, our files contained information used to prepare tax returns, which may have included your name, address, Social Security number, wage information, and bank account information if you provided it.

Attribution 1 Publication: NY AG's office Author:
Article Title: Jaffa Simmons PLLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-16	**Hospital Housekeeping Systems**	TX	9/8/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**1,058**

During the course of the investigation, we determined that our IT systems were not affected and our payroll provider indicated that their systems were not affected. However, on August 19, 2017, we identified a targeted spear phishing email message that had been sent to a HHS employee on March 8, 2016.

Attribution 1 Publication: NY AG's office Author:
Article Title: Hospital Housekeeping Systems
Article URL: per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-14	**Franklin American Mortgage Company**	TN	8/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**2,196**

Some of your personal information was included in a boxed shipment that was sent to PNC, where your loan servicing was transferred in April 2017. Your personal information included in boxes may have included your name, address, Social Security Number, and account.

Attribution 1 Publication: NY AG's office Author:
Article Title: Franklin American Mortgage Company
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-13	**Farmers Insurance**	CA	8/22/2017	Electronic	Business	Yes - Published #	**705**

I am writing to let you know that Farmers Insurance® was notified by the U.S. Postal Inspector that in the course of an investigation, an electronic device belonging to an employee of one of our vendors was recovered. As a result, Farmers Insurance undertook an exploratory investigation and determined that while the device did not contain your personal information, evidence showed the vendor's employee gained unauthorized access to Farmers systems that contained your personal information, obtained during the normal course of business to service a policy or policies that you acquired or sought to acquire from Farmers.

Attribution 1 Publication: NY AG's office Author:
Article Title: Farmers Insurance
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-12	**Farmers & Merchants Bank**	VA	9/21/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**10,650**

On July 25, 2017, we learned that the email accounts of two of our employees had been compromised. The account contained certain personal information including names, Social Security numbers and, for some individuals, a bank account number and/or driver's license number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Farmers & Merchants Bank
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-11	Fairway Westbury LLC	NY	8/2/2017	Electronic	Business	Yes - Published #	4,360

We are writing to let you know about an issue that may involve your personal information. We recently discovered a skimming device on a point of sale card reader at the Fairway Market store located in Westbury, New York. You are receiving this letter because your name and payment card information may have been compromised.

Attribution 1 Publication: NY AG's office Author:
Article Title: Fairway Westbury LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-10	Fairway Douglaston LLC	NY	8/2/2017	Electronic	Business	Yes - Published #	3,720

We are writing to let you know about an issue that may involve your personal information. We recently discovered a skimming device on a point of sale card reader at the Fairway Market store located in Douglaston, New York. You are receiving this letter because your name and payment card information may have been compromised.

Attribution 1 Publication: NY AG's office Author:
Article Title: Fairway Douglaston LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-09	Fairway Pelham LLC	NY	8/2/2017	Electronic	Business	Yes - Published #	1,750

We are writing to let you know about an issue that may involve your personal information.We recently discovered a skimming device on a point of sale card reader at the Fairway Market store located in Peham, New York. You are receiving this letter because your name and payment card information may have been compromised.

Attribution 1 Publication: NY AG's office Author:
Article Title: Fairway Pelham LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-08	Fairway Chelsea LLC	NY	8/2/2017	Electronic	Banking/Credit/Financial	Yes - Published #	3,887

We recently discovered a skimming device on a point of sale card reader at the Fairway Market store located in the Chelsea neighborhood of Manhattan. We recently discovered a skimming device on a point of sale card reader at the Fairway Market store located in the Chelsea neighborhood of Manhattan. You are receiving this letter because your name and payment card information may have been compromised.

Attribution 1 Publication: NY AG's office Author:
Article Title: Fairway Chelsea LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-07	Eastern Jungle Gym, Inc.	NY	7/31/2017	Electronic	Business	Yes - Published #	1,900

While performing a security update to our website, www.eastemjunglegym.com, it was discovered that unauthorized individuals may have obtained payment information that was keyed into the checkout process. The potentially-affected information includes credit card numbers, expiration dates, and card verification codes for orders processed on www.easternjunglegym.com between February 20th, 2017 and June 21st, 2017.

Attribution 1 Publication: NY AG's office Author:
Article Title: Eastern Jungle Gym, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-06	Way.com	CA	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	3,057

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Way.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-05	Walk in the Word-e com	IL	9/28/2017	Electronic	Banking/Credit/Financial	Yes - Published #	1,332

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Walk in the Word-e com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-04	Villa JTM Internet Sales	PA	9/28/2017	Electronic	Banking/Credit/Financial	Yes - Published #	1,503

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Villa ITM Internet Sales
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-03	Trump Hotels	FL	8/10/2017	Electronic	Banking/Credit/Financial	Yes - Published #	553

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Trump Hotels
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-02	Ben's Deli	NY	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	444

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Ben's Deli
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171231-01	Dutchess Boces	NY	12/31/2017	Electronic	Banking/Credit/Financial	Yes - Published #	400

I am writing to apologize for inadvertently posting members' social security numbers as part of a seniority list shared at the Alternative Hitfh School (BETA).

Attribution 1 Publication: NY AG's office Author:
Article Title: Dutchess Boces
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-99	**Curriculum Associates, LLC**	MA	8/14/2017	Electronic	Business	Yes - Published #	**102**

Per Notification NY AG's office
Description of Breach: Hacking/phishing
Information Acquired: SSN and driver's license number or non-driver identification card number

Attribution 1 Publication: NY AG's office Author:
Article Title: Curriculum Associates, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-98	**Covanta Holding Corporation**	NJ	7/14/2017	Electronic	Business	Yes - Published #	**258**

On April 21. 2017, we learned that a "phishing" email message was sent from outside the company to certain employees on April 17th. Not all employees who received the phishing email opened it. For those employees who opened the email, the information potentially affected was W-2 information, including name, address, Social Security number, earnings, bank account and routing number.

Attribution 1 Publication: NY AG' office Author:
Article Title: Covanta Holding Corporation
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-97	**Coatings & Adhesives Corporation**	NC	7/20/2017	Electronic	Business	Yes - Published #	**189**

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Coatings & Adhesives Corporation
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-96	**Eagle Home Mortgage, LLC f/k/a Universal American**	FL	7/24/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**374**

Per Notification NY AG's office
Description of Breach: Unauthorized access
Information Acquired: Financial information, SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Eagle Home Mortgage, LLC f/k/a Universal American Mortgage Co. LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-95	**Lewis Management Corp.**	CA	8/23/2017	Electronic	Business	Yes - Published #	**309**

Per Notification NY AG's office
Description of Breach: Insider wrongdoing
Information Acquired: Driver's license number or non-driver identification card.

Attribution 1 Publication: NY AG's office Author:
Article Title: Lewis Management Corp.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-94	**Brambles USA Inc.**	GA	9/15/2017	Electronic	Business	Yes - Published #	**105**

Specifically, a number of Recycled employees received a phishing email claiming to set out an “Organisational Notice” from Brambles’ CEO. This included your social security number, your date of birth, and, to the extent you had provided it previously, your banking information (only the last 4 digits of your routing number).

Attribution 1 Publication: NY AG's office Author:
Article Title: Brambles USA Inc.
Article URL: Per FOIL NY AG’s office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-93	**Attarson & Associates, Inc.**	CA	8/17/2017	Electronic	Business	Yes - Published #	**184**

On June 14, 2017, we discovered that your tax information stored on our server may have been accessed by an unknown, unauthorized third-party. Although the investigation has not identified evidence that your information was actually compromised, it is possible that your name, address, Social Security number and tax information may have been obtained by an unauthorized third-party.

Attribution 1 Publication: NY AG’s office Author:
Article Title: Attarson & Associates, Inc.
Article URL: Per FOIL NY AG’s office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-92	**American Financial Network Advisory Services, LLC**	CA	8/8/2017	Electronic	Business	Yes - Published #	**133**

Per Notification NY AG’s office
Description of Breach: External systems breach
Information Acquired: SSN

Attribution 1 Publication: NY AG’s office Author:
Article Title: American Financial Network Advisory Services, LLC
Article URL: Per FOIL NY AG’s office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-90	**Middlesex Corporation**	MA	7/1/2017	Electronic	Business	Yes - Published #	**1,041**

Per Notification NY AG’s office
Description of Breach: hacking / phishing
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Middlesex Corporation
Article URL: Per FOIL NY AG’s office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-89	**Fiduciary Group**	GA	7/1/2017	Electronic	Business	Yes - Published #	**331**

On March 24, 2017, TFG learned that a targeted ?phishing? email had been sent to a TFG employee. Believing the email to be legitimate, the TFG employee responded and, in the process, disclosed the employeees email login. After a detailed and thorough analysis of the data, TFG's investigation determined that some personal information, including names, Social Security number, and investment account numbers, was accessible to the unauthorized party.

Attribution 1 Publication: NY AG's office Author:
Article Title: Fiduciary Group
Article URL: Per FOIL NY AG’s office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-88	VHG Fourth Street SF, LLC	CA	7/1/2017	Electronic	Business	Yes - Published #	280

Per Notification NY AG's office
Description of Breach: Theft of device, documentation or media
Information Acquired: Financial information (account number or credit/debit card number, in combination with the security code, password, or PIN for the account

Attribution 1 Publication: NY AG's office Author:
Article Title: VHG Fourth Street SF, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-87	Valmark Securities	OH	7/1/2017	Electronic	Business	Yes - Published #	120

Per Notification NY AG's office
Description of Breach: External systems breach (hacking)
Information Acquired: SSN and financial information (account number or credit/debit card number, in combination with the security code, password, or PIN for the account

Attribution 1 Publication: NY AG's office Author:
Article Title: Valmark Securities
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-86	Torchon & Associates	CA	7/1/2017	Electronic	Business	Yes - Published #	503

Per Notification NY AG's office
Description of Breach: hacking
Information Acquired: SSN and financial accout number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account.

Attribution 1 Publication: NY AG's office Author:
Article Title: Torchon & Associates
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-85	Santander Bank (4/24)	MA	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	204

Santander Bank is strongly committed to the security of our cardholders' information and strives to let you know about security concerns as soon as possible. We are writing to notify you of a data security incident that occurred at the ATM located at <ATM Location> on <Month> <Day>, <Year> involving your Santander® Card. As a result of this incident, we have reason to believe the following information was compromised:
• Your name • Card number • Personal Identification Number (PIN). and
• Card expiration date.

Attribution 1 Publication: NY AG's office Author:
Article Title: Santander Bank (4/24)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-84	Santander Bank (5/1)	MA	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	139

Santander Bank is strongly committed to the security of our cardholders' information and strives to let you know about security concerns as soon as possible. We are writing to notify you of a data security incident that occurred at the ATM located at <ATM Location> on <Month> <Day>, <Year> involving your Santander® Card.

Attribution 1 Publication: NY AG's office Author:
Article Title: Santander Bank (5/1)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-83	Santander Bank (5/23)	MA	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	153

Santander Bank is strongly committed to the security of our cardholders' information and strives to let you know about security concerns as soon as possible. We are writing to notify you of a data security incident that occurred at the ATM located at <ATM Location> on <Month> <Day>, <Year> involving your Santander® Card. As a result of this incident, we have reason to believe the following information was compromised:
• Your name • Card number • Personal Identification Number (PIN). and
• Card expiration date.

Attribution 1 Publication: NY AG's office Author:
Article Title: Santander Bank (5/23)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-82	Zoo Atlanta	GA	7/1/2017	Electronic	Business	Yes - Published #	411

On March 1, 2017, the Zoo learned that a Zoo email address had been hacked. The Zoo worked swiftly to lock the hacker out of that account and to confirm that this was an isolated occurrence and that no other employee's e-mail account was impacted. As a result of this incident, the 2016 W-2 information, including name and Social Security number, of Zoo employees was compromised.

Attribution 1 Publication: NY AG's office Author:
Article Title: Zoo Atlanta
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-81	TDX Construction Corporation	NY	7/1/2017	Electronic	Business	Yes - Published #	193

We have just leamed that in early February, 2017, some employee personal information was inadvertently disclosed to a third party as a result of an effective e-mail "phishing scam·. The data that was accessed included personal information, such as your Address, Social Security Number and W-2 information.

Attribution 1 Publication: NY AG's office Author:
Article Title: TDX Construction Corporation
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-80	Tyler Devices	NV	7/1/2017	Electronic	Business	Yes - Published #	128

On February 9, 2017, Taylor Devices, Inc. became aware that a copy of 2016 W-2 information for 128 employees/former employees was erroneously emailed to an imposter claiming to be senior management
of the company. The W-2 form contains personal information including wage and social security number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Tyler Devices
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-79	Collier Companies	FL	7/1/2017	Electronic	Business	Yes - Published #	317

On January 26, 2017, The Collier Companies discovered that, in connection with a lease signing that may have occurred since March 2015, some of your personal information contained in certain lease-related documents could have been accessed when a link to a secured document portal was inadvertently sent to an incorrect e-mail address that was similar to your e-mail address. Those lease-related documents contained your name, address, date of birth, driver's license number and Social Security number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Collier Companies
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-78	TradingScreen Inc.	NY	7/1/2017	Electronic	Business	Yes - Published #	114

On February 2, one of our employees received an email that was carefully crafted to appear to be from a senior company officer. The email asked the employee to send back copies of the IRS W-2 forms of all US employees to the sender of the email. Thinking that the email was a legitimate request from an authorized company officer for necessary information, the employee sent a response via email with a PDF file containing the requested W-2 forms.

Attribution 1 Publication: NY AG's office Author:
Article Title: TradingScreen Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-77	Susan D. Jarvis, CPA	PA	7/1/2017	Electronic	Business	Yes - Published #	316

Earller this month, I discovered that our firm was the victim of a cyber Intrusion by which an unknown third party was able to access my computer network and some of my cllents' personal Information. As a result, some of your personal Information may have been exposed to others, including your first and last name, home address, social security number, and 2015 compensation data.

Attribution 1 Publication: NY AG's office Author:
Article Title: Susan D. Jarvis, CPA
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-76	Suffolk County National Bank	NY	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	191

Per Notification NY AG's office
Description of Breach: ATM Skimmer
Information Acquired: credit/debit card

Attribution 1 Publication: NY AG's office Author:
Article Title: Suffolk County National Bank
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-75	St. Lucie County	FL	7/1/2017	Electronic	Government/Military	Yes - Published #	3,859

On March 9, 2017, St. Lucie County learned that individuals accessing court records on its website may have been able to inadvertently view confidential information typically accessible only to County staff.
Our investigation has determined that some of your information could have been accessible to unauthorized individuals and may have included your name, date of birth, Social Security number, and the results of your court-ordered drug testing.

Attribution 1 Publication: NY AG's office Author:
Article Title: St. Lucie County
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-74	SKE Group	NJ	7/1/2017	Electronic	Business	Yes - Published #	442

We are writing to inform you of a potential data security incident that may have resulted in the disclosure of your minor's personal information, including your name, address, birth date, Social Security number, and financial account information.

Attribution 1 Publication: NY AG's office Author:
Article Title: SKE Group
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-73	Shiel Medical Laboratory	NY	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	150

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Shiel Medical Laboratory
Article URL: Per FOIl NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-72	Scientific Games Corporation	NV	7/1/2017	Electronic	Business	Yes - Published #	280

Per Notification NY AG's office
Description of Breach: loss or theft of device
Information Acquired: SSN and Driver's License

Attribution 1 Publication: NY AG's office Author:
Article Title: Scientific Games Corporation
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-70	Shared Imaging	IL	7/1/2017	Electronic	Business	Yes - Published #	197

Per Notification NY AG's office
Description of Breach: Email spoofing
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Shared Imaging
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-69	Revlon Consumer Products Corporation	NY	7/1/2017	Electronic	Business	Yes - Published #	149

Per Notification NY AG's office
Description of Breach: loss or theft of device or media (e.g. computer, laptop, external hard drive, thumb drive, CD, tape)
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Revlon Consumer Products Corporation
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-68	Rising Tide Charter Public School	MA	7/1/2017	Electronic	Educational	Yes - Published #	272

On February 13, 2017, we discovered that cyber attackers may have gained unauthorized access to information stored on a computer server utilized by the School. The information potentially accessed may have included your name, address, date of birth and Social Security Number

Attribution 1 Publication: NY AG's office Author:
Article Title: Rising Tide Charter Public School
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-67	Rammelkamp Bradney PC	IL	7/1/2017	Electronic	Business	Yes - Published #	418

Per Notification NY AG's office
Description of Breach: External system breach (e.g. hacking)
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Rammelkamp Bradney PC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-66	Reid, Sahm, Isaacs & Schmelzlen LLP	CA	7/1/2017	Electronic	Business	Yes - Published #	379

Over the past month we became aware that some of our clients had received an e-mail that appeared to be from our office, but was in fact a "spoofed" e-mail (i.e., not actually from our office and from an unauthorized and unrelated Gmail account). This information may have included your W-2 or Form 1099.

Attribution 1 Publication: NY AG's office Author:
Article Title: Reid, Sahm, Isaacs & Schmelzlen LLP
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-65	Continental American Insurance Company	SC	7/1/2017	Electronic	Business	Yes - Published #	675

Per Notification NY AG's office
Description of Breach: External breach (e.g. hacking)
Information Acquired: SSN and Financial account number or credit or debit card number, in combination with the security code, access code (not clearly defined)

Attribution 1 Publication: NY AG's office Author:
Article Title: Continental American Insurance Company
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-64	Advanced ICU Care, Inc.	MO	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	320

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Advanced ICU Care, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-63	Bedlam Theater	NY	7/1/2017	Electronic	Business	Yes - Published #	109

Per Notification NY AG's office
Description of Breach: Loss or theft of device or media
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Bedlam Theater
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-62	**Union Square Hospitality Group**	NY	7/1/2017	Electronic	Business	Yes - Published #	**989**

Per Notification NY AG's office
Description of Breach: Loss or theft of device or media
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Union Square Hospitality Group
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-61	**United Church Homes**	OH	7/1/2017	Electronic	Business	Yes - Published #	**2,020**

On March 15, 2017, UCH was the target of an e-mail phishing attack that resulted in the disclosure of certain of its employees' 2016 IRS Form W-2s, Wage and Tax Statements which included the affected employees' first and last names, addresses, Social Security numbers and compensation information.

Attribution 1 Publication: NY AG's office Author:
Article Title: United Church Homes
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-60	**Country Mutual Insurance Company**	FL	7/1/2017	Electronic	Business	Yes - Published #	**3,272**

Per Notification NY AG's office
Description of Breach: Insider wrongdoing
Information Acquired: Driver's license

Attribution 1 Publication: NY AG's office Author:
Article Title: Country Mutual Insurance Company
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-59	**Granite Services, Inc.**	FL	7/1/2017	Electronic	Business	Yes - Published #	**111**

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Granite Services, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-58	**Masschusetts Higher Education Assistance**	MA	7/1/2017	Electronic	Business	Yes - Published #	**323**

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Masschusetts Higher Education Assistance Corporation dba American Student Assistance
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-57	Mi9 Retail	FL	7/1/2017	Electronic	Business	Yes - Published #	127

On January 30, 2017 we discovered that earlier that same day, as a result of a criminal phishing email, an unauthorized third party obtained an electronic file containing 2016 Form W-2s of certain current and former employees of Mi9 Retail.

Attribution 1 Publication: NY AG's office Author:
Article Title: Mi9 Retail
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-56	Marrakech	CT	7/1/2017	Electronic	Business	Yes - Published #	1,656

On January 24, 2017, Marrakech was subject to a sophisticated phishing attack. An employee in the payroll department received a spoofed email that purported to be from the CEO. That email requested W-2 information for 2015 and 2016. Believing that the email actually came from Marrakech's CEO, the requested information was sent. The phisher was also provided logon information to a website containing W-2 information.

Attribution 1 Publication: NY AG's office Author:
Article Title: Marrakech
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-55	Maison Gerard Ltd.	NY	7/1/2017	Electronic	Business	Yes - Published #	607

Between December 22, 20l6 and January 2, 2017, while it was closed for the holiday, the gallery suffered a break-in. The data accessed likely included client names and addresses, the last 4 digits of any credit card you may have used to purchase an item from the gallery. copies of any checks the gallery received from you for payment of a purchased item, which check would include the bank account and routing number and your signature, as well as a copy of any resale certificates you may have provided to the gallery.

Attribution 1 Publication: NY AG's office Author:
Article Title: Maison Gerard Ltd.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-54	Long Island University	NY	7/1/2017	Electronic	Educational	Yes - Published #	3,877

On January 2, 2017 a file with undergraduate student information was inadvertently emailed to some LIU undergraduate students.The inadvertent disclosure contained names, birth dates and addresses that in theory could have been used to test passwords on student accounts.

Attribution 1 Publication: NY AG's office Author:
Article Title: Long Island University
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-53	Liberty Pumps	NY	7/1/2017	Electronic	Business	Yes - Published #	400

We have been informed that our third-party cloud services provider was the victim of a malware incident. The data potentially exposed may include user first and last name; phone number: zip code; email address; NightEye• account password; device ID number; and event notification history.

Attribution 1 Publication: NY AG's office Author:
Article Title: Liberty Pumps
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-52	Kayser-Roth Inc.	NC	7/1/2017	Electronic	Business	Yes - Published #	10,767

Per Notification NY AG's office
Description of Breach: External systems breach
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Kayser-Roth Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-51	Katherine Siemionko / Women's March on NYC	NY	7/1/2017	Electronic	Business	Yes - Published #	49,000

Per Notification NY AG's office
Description of Breach: insider wrongdoing
Information Acquired: unspecified

Attribution 1 Publication: NY AG's office Author:
Article Title: Katherine Siemionko / Women's March on NYC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-50	Jetpay Corporation	PA	7/1/2017	Electronic	Business	Yes - Published #	367

Per Notification NY AG's office
Description of Breach: Unauthorized access
Information Acquired: SSN and credit/debit card number

Attribution 1 Publication: NY AG's office Author:
Article Title: Jetpay Corporation
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-49	InMotion Hosting, Inc	VA	7/1/2017	Electronic	Business	Yes - Published #	368

On January 25, 2017, InMotion Hosting, Inc. ("InMotion") learned it was the target of an email phishing scheme which resulted in unauthorized access to forms which contained your personal information including name, address, Social Security number, and compensation information.

Attribution 1 Publication: NY AG's office Author:
Article Title: InMotion Hosting, Inc
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-48	Wet n Wild Beauty	y	7/1/2017	Electronic	Business	Yes - Published #	896

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Wet n Wild Beauty
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-47	Vaporseller	FL	7/1/2017	Electronic	Business	Yes - Published #	101

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Vaporseller
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-46	**Rubber Stamp End Button Champ**	CA	7/1/2017	Electronic	Business	Yes - Published #	**634**

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Rubber Stamp End Button Champ
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-45	**www.therafitshoe.com**	FL	7/1/2017	Electronic	Business	Yes - Published #	**150**

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: www.therafitshoe.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-44	**Guardian Technologies**	OH	7/1/2017	Electronic	Business	Yes - Unknown #	**Unknown**

The company that manages our website informed us on April 26, 2017 that portions of the code on Guardian Technologies' website had been modified so certain customer information was transmitted to unknown parties while online transactions were being processed.

Attribution 1 Publication: NY AG's office Author:
Article Title: Guardian Technologies
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-43	**Wilderness Hotel and Resort**	WI	7/1/2017	Electronic	Business	Yes - Published #	**2,085**

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Wilderness Hotel and Resort
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-42	**Wise Company Inc.**	UT	7/1/2017	Electronic	Business	Yes - Published #	**3,355**

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Wise Company Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-41	Experian Information Solutions	CA	7/1/2017	Electronic	Business	Yes - Published #	619

Per Notification NY AG's office
Description of Breach: Other / unauthorized access
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Experian Information Solutions
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-40	Edgewood Management Corp.	MD	7/1/2017	Electronic	Business	Yes - Published #	1,873

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

Attribution 1 Publication: NY AG's Office Author:
Article Title: Edgewood Management Corp.
Article URL: Per FOIL NY AG's Office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-39	Funding Circle USA, Inc.	CA	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	3,508

Per Notification NY AG's office
Description of Breach: Unauthorized Access (not including theft. Loss or hacking)
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Funding Circle USA, Inc.
Article URL: Per FOIL NY AG's Office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-38	Hewlett-Woodmere Public Schools	NY	7/1/2017	Electronic	Educational	Yes - Published #	446

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Hewlett-Woodmere Public Schools
Article URL: Per FOIL NY AG's Office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-37	Honest Weight Food Co-Op	NY	7/1/2017	Electronic	Business	Yes - Published #	275

On October 18, 2016, Honest Weight became aware of unauthorized remote connections to computer systems in our network. Because we value our relationship with you, we wanted to make you aware of this incident because the unauthorized party may have accessed some of your personal information within the infected server, including your full name, Social Security number and date of birth. This incident was limited to employee information only.

Attribution 1 Publication: NY AG's Office Author:
Article Title: Honest Weight Food Co-Op
Article URL: Per FOIL NY AG's Office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-36	haixiaq zhang	CA	7/1/2017	Electronic	Business	Yes - Published #	765

Per Notification NY AG's office
Description of Breach: W2 Phishing Scam
Information Acquired: SSN

Attribution 1 Publication: NY AG's Office Author:
Article Title: haixiaq zhang
Article URL: Per FOIL NY AG's Office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-35	DirectPath, LLC / Ensemble Health Partners	AL	7/1/2017	Electronic	Business	Yes - Published #	639

On May 26, 2017, a DirectPath employee's bag containing the employee's laptop was stolen from the employee's personal car while it was parked off DirectPath's premises. Immediately following the report of the theft, DirectPath undertook a thorough investigation, which revealed that the laptop was password protected and contains personal information, including your name and Social Security number.

Attribution 1 Publication: NY AG's office Author:
Article Title: DirectPath, LLC / Ensemble Health Partners
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-34	Equian LLC (May)	IN	7/1/2017	Electronic	Business	Yes - Published #	299

On or about March 29, 2017, we discovered that on August 23, 2016, an unauthorized third party may have received access to 2015 W-2 tax information for current and former Equian employees through a phishing email scam. The information contained in the W-2 tax forms included employees' first and last names, addresses, and Social Security numbers.

Attribution 1 Publication: NY AG's office Author:
Article Title: Equian LLC (May)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-33	Empire International, Empire Chauffeur Services, Ltd. And	NJ	7/1/2017	Electronic	Business	Yes - Published #	897

Regrettably, we are writing to inform you of a sophisticated email
phishing incident that occurred on January 26, 2017 that involved disclosure of your W-2 information, which included your name, address, Social Security number and income information. No bank account or direct deposit information was included.

Attribution 1 Publication: NY AG's office Author:
Article Title: Empire International, Empire Chauffeur Services, Ltd. And Securecar, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-32	Golomb, Schwartz & Cove, PA	FL	7/1/2017	Electronic	Business	Yes - Published #	1,253

On March 20, 2017, the forensic investigation concluded that an unauthorized third party had accessed our computer server, beginning on March 4, 2016, and subsequently appeared to have obtained certain client information, including your full name, address and Social Security number. Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Golomb, Schwartz & Cove, PA
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-31	Hajek & Hajek CPA's, PA	FL	7/1/2017	Electronic	Business	Yes - Published #	155

Per Notification NY AG's office
Description of Breach: Hacking
Information Acquired: Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account.

Attribution 1 Publication: NY AG's office Author:
Article Title: Hajek & Hajek CPA's, PA
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-30	Hamillton Central School District	NY	7/1/2017	Electronic	Educational	Yes - Published #	570

It has come to our attention that an individual (former employee) has unlawfully accessed, and may have downloaded or otherwise copied, sensitive information belonging to approximately 10 district students, including their names, identification numbers, class schedules and grades.

Attribution 1 Publication: NY AG's office Author:
Article Title: Hamillton Central School District
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-29	Harmonix Music Systems, Inc.	MA	7/1/2017	Electronic	Business	Yes - Published #	154

On May 31, 2017, the Company discovered that on February 17, 2017. a Harmonix employee had received a targeted "spear phishing" email that had been disguised to appear as though it had been sent by another Harmonix employee, requesting employees' 2016 W-2 information. The information that was disclosed to the unauthorized third party included employees' names, addresses, Social Security numbers, employee identification numbers, salary information, information related to tax withholdings and employee benefits, and the employee's department.

Attribution 1 Publication: NY AG's office Author:
Article Title: Harmonix Music Systems, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-28	Thomas E. Strauss, Inc.	PA	7/1/2017	Electronic	Business	Yes - Published #	406

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Thomas E. Strauss, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-27	Tennis Express	TX	7/1/2017	Electronic	Business	Yes - Published #	7,117

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Tennis Express
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-26	socksaddicts.com	MI	7/1/2017	Electronic	Business	Yes - Published #	1,007

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: socksaddicts.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-25	Silencer Shop	TX	7/1/2017	Electronic	Business	Yes - Published #	628

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Silencer Shop
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-24	Shoney's	TN	7/1/2017	Electronic	Business	Yes - Published #	125

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Shoney's
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-23	Rough Country	TN	7/1/2017	Electronic	Business	Yes - Published #	559

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Rough Country
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-22	Restaurants Unlimited, Inc.	CA	7/1/2017	Electronic	Business	Yes - Published #	316

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Restaurants Unlimited, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-21	Schlitz & Giggles Perkins	LA	7/1/2017	Electronic	Business	Yes - Published #	137

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Schlitz & Giggles Perkins
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-20	OCR Integrator	KY	7/1/2017	Electronic	Business	Yes - Published #	248

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: OCR Integrator
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-19	PiketoPeak.com	MI	7/1/2017	Electronic	Business	Yes - Published #	172

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: PiketoPeak.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-18	Pictureframes.com	NC	7/1/2017	Electronic	Business	Yes - Published #	567

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Pictureframes.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-17	Photobarn Photo Lab	TN	7/1/2017	Electronic	Business	Yes - Published #	1,496

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Photobarn Photo Lab
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-16	Peg Leg Petes	FL	7/1/2017	Electronic	Business	Yes - Published #	537

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Peg Leg Petes
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-15	Opentip.com	MA	7/1/2017	Electronic	Business	Yes - Published #	1,583

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Opentip.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-14	Ocean Key House Resort	FL	7/1/2017	Electronic	Business	Yes - Published #	321

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Ocean Key House Resort
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-13	Natural News Store	WY	7/1/2017	Electronic	Business	Yes - Published #	441

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Natural News Store
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-12	National Furniture Supply	GA	7/1/2017	Electronic	Business	Yes - Published #	229

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: National Furniture Supply
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-11	Love Book LLC	MI	7/1/2017	Electronic	Business	Yes - Published #	610

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Love Book LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-10	Lions-Pride.com	y	7/1/2017	Electronic	Business	Yes - Published #	331

Per FOIL NY AG's office

Attribution 1 Publication: Lions-Pride.com Author:
Article Title: Lions-Pride.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-09	Life Supports Depot	CA	7/1/2017	Electronic	Business	Yes - Published #	127

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Life Supports Depot
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-08	Nathan Associates Inc.	VA	7/1/2017	Electronic	Business	Yes - Published #	168

On or about March 17, 2017, Nathan Associates became aware that a former employee emailed 401 (k) participant information outside of the company In an unauthorized manner while stillemployed by the company. The emails were sent on December 29 and 30, 2016 and contained employee personal information, including Social Security numbers

Attribution 1 Publication: NY AG's office Author:
Article Title: Nathan Associates Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-07	JPW Industries	TN	7/1/2017	Electronic	Business	Yes - Published #	175

On May 9, 2017, we learned that a former employee conducted an unauthorized release of certain confidential information in response to a phishing email. As a result of this incident we learned that an unauthorized individual may have obtained IRS Form W-2s for the 2016 employment year for you and other employees on January 17, 2017.

Attribution 1 Publication: NY AG's office Author:
Article Title: JPW Industries
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-06	Jas. Townsend & Son, Inc.	IN	7/1/2017	Electronic	Business	Yes - Published #	1,813

The incident appears to have occurred as a result of an unauthorized party gaining access to certain customer data during data transfer to our credit card processor. The incident caused certain secured personal information, including name, address, credit and/or debit card account number. and credit and/or debit card security codes to be potentially exposed to unauthorized individuals.

Attribution 1 Publication: NY AG's office Author:
Article Title: Jas. Townsend & Son, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-05	Jackson Hewitt	NJ	7/1/2017	Electronic	Business	Yes - Published #	77,178

Specifically, in February 2017 we identified what appeared to be unusual system activity. However, the personal information may have included names, addresses, telephone numbers, email addresses, social security numbers, taxpayer identification numbers, driver's license or other government identification numbers, bank account numbers and other tax-return preparation related information, including backup or supporting documentation.

Attribution 1 Publication: NY AG's office Author:
Article Title: Jackson Hewitt
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-04	Jade Bloom	UT	7/1/2017	Electronic	Business	Yes - Published #	251

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Jade Bloom
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-03	Jewelry.com	FL	7/1/2017	Electronic	Business	Yes - Published #	6,962

On May 16, 2017 Jewelry.com discovered that, beginning on or about November 16, 2016, unknown individuals gained access to our online boutique through the unauthorized use of an account belonging to one of our employees. (Exposure number per NY AG's office)

Attribution 1 Publication: NY AG's office Author:
Article Title: Jewelry.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-02	Lanier Parking	GA	7/1/2017	Electronic	Business	Yes - Published #	1,811

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Lanier Parking
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171230-01	Immersion Consulting	MD	7/1/2017	Electronic	Business	Yes - Published #	142

Per FOIL NY AG's Office
Description of Breach: Inadvertent disclosure
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Immersion Consulting
Article URL: Per FOIL NY AG's office

Attribution 2 Publication: NY AG's Office Author:
Article Title: Immersion Consulting
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-48	Mercer LLC	NY	7/1/2017	Electronic	Business	Yes - Published #	Unknown

Mercer has informed NYSE that a former Mercer employee changed your password used to access the website without authorization. Mercer believes that the former employee was able to view your name, address, phone number, birth date, Social Security Number, and the financial account into which you decided pension payments will be made, as well as the identity and personal information you provided regarding your beneficiary.

Attribution 1 Publication: NY AG's office Author:
Article Title: Mercer LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-47	Horseshoe Hammond, LLC dba Horseshoe Casino	IN	8/30/2017	Electronic	Business	Yes - Published #	272

We recently discovered that an employee may have accessed and used your information to apply for a Total Rewards® Visa card without permission. It is possible this employee accessed and used your name, address, phone number, date of birth, and social security number to apply without your permission.

Attribution 1 Publication: NY AG's office Author:
Article Title: Horseshoe Hammond, LLC dba Horseshoe Casino Hammond
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-46	Caesars Entertainment	NV	9/1/2017	Electronic	Business	Yes - Published #	162

On August 15, 2017, we became aware of suspicious Total Rewards account activity and immediately began an investigation. During the investigation, we discovered that your name, Total Rewards account number, online usernanme and/or online password may have been viewed and used to redeem your Reward Credits for electronic gift cards from the Total Rewards online catalog without your permission.

Attribution 1 Publication: NY AG's office Author:
Article Title: Caesars Entertainment
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-45	Freeport Public Schools	NY	7/1/2017	Electronic	Educational	Yes - Published #	120

Per Notification NY AG's office
Description of Breach: external system breach
Information Acquired: undefined

Attribution 1 Publication: NY AG's office Author:
Article Title: Freeport Public Schools
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-44	Republic Bank & Trust Company	KY	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	32,649

Per Notification NY AG's office
Description of Breach: External system breach
Information Acquired: SSN and Driver's license

Attribution 1 Publication: NY AG's office Author:
Article Title: Republic Bank & Trust Company
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-43	Capital One (5/9)	VA	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	348

Based on one of our regular reviews of your aocount(s) for fraud, we suspect that someone successfully logged in to your account(s) using your username and password, which we believe was stolen from one of these websites. We believe that <AdhocVar2>, the fraudster had access to your Capital One account information, which may include your name, address, full or partial account number and transaction history.

Attribution 1 Publication: NY AG's office Author:
Article Title: Capital One (5/9)
Article URL: Per Foil NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-42	First National Bank of Pennsylvania (4/7)	PA	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	9,358

Per Notification NY AG's office
Description of Breach: External systems breach
Information Acquired: SSN and Driver's license

Attribution 1 Publication: NY AG's office Author:
Article Title: First National Bank of Pennsylvania (4/7)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-41	NextGen Global Resources	IL	11/12/2017	Electronic	Business	Yes - Unknown #	Unknown

On November 12, 2017, we discovered that an employee had inadvertently responded to a phishing attack email, allowing an unauthorized person to create an email rule in that employee's email account automatically forwarding incoming email to an unknown third party. You are receiving this notice because your name and your social security number was included in one of these two scenarios.

Attribution 1 Publication: NY AG's office / CA AG's office Author:
Article Title: NextGen
Article URL: https://oag.ca.gov/ecrime/databreach/reports/sb24-131689

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-40	Capital One (8/25)	VA	8/25/2017	Electronic	Banking/Credit/Financial	Yes - Published #	208

We originally notified you on August 22, 20 17. In July 2017, an internal investigation revealed a Capital One, N.A. ("Capital One") employee inappropriately emailed some customers' personal information, from May 19, 2015 through March 25, 2017. The non-public personal information contained within the emails includes name, address, account number, Social Security Number, date of birth, email address, telephone number and/or transaction history.

Attribution 1 Publication: NY AG's office Author:
Article Title: Capital One (8/25)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-39	Capital One (9/21)	VA	9/21/2017	Electronic	Banking/Credit/Financial	Yes - Published #	1,267

We recently detected suspicious activity related to your Capital One® online credentials. We believe that <AdhocVar2>, the fraudster had access to your Capital One account information. which may include your name, address. full or partial account number and transaction history.

Attribution 1 Publication: NY AG's office Author:
Article Title: Capital One (9/21)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-38	Fate Therapeutics, Inc.	CA	7/12/2017	Electronic	Medical/Healthcare	Yes - Published #	177

Per Notification NY AG's office
Description of Breach: unauthorized access
Information Acquired: SSN

Attribution 1 Publication: NY AG's office Author:
Article Title: Fate Therapeutics, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-37	Dr. Richard M. Hooley, District Superintendent	NY	10/20/2017	Electronic	Educational	Yes - Published #	150

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

Attribution 1 Publication: NY AG's office Author:
Article Title: Dr. Richard M. Hooley, District Superintendent
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-36	Gomerdinger & Associates	CO	7/3/2017	Electronic	Business	Yes - Published #	289

On May 19, 2017 we discovered that on May 11, 2017 an unauthorized third party obtained access to electronic files containing tax documents. including tax renirns of some clients of Gomerdinger and Associates.
We have confirmed that the information obtained by the unauthorized party included your tax documents, which included your full name. Social Security number, bank account information. home address. and possibly your driver's license number if you supplied it to us.

Attribution 1 Publication: NY AG's office Author:
Article Title: Gomerdinger & Associates
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-35	Firstservice Residential New York, Inc.	NY	7/7/2017	Electronic	Business	Yes - Published #	142

We are contacting you regarding a data security incident that occurred in April 2017 within the email account of a FirstService Residential associate who is involved in the activities of [Name or address of property]. Unauthorized parties may have accessed your personal identifiable information (i.e., your name, account or Social Security number).

Attribution 1 Publication: NY AG's office Author:
Article Title: Firstservice Residential New York, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-34	Horchow Collection	TX	7/1/2017	Electronic	Business	Yes - Published #	1,123

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Horchow Collection
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-33	Growmark FS, LLC	DE	9/1/2017	Electronic	Business	Yes - Published #	144

On July 2, 2017, a GROWMARK employee discovered that the employee's laptop had been stolen out of their car overnight. The personal information that was saved to the laptop was a combination of the individuals' name and one or more of their Social Security nwnber, driver's license number or bank account nunber.

Attribution 1 Publication: NY AG's office Author:
Article Title: Growmark FS, LLC
Article URL: Per NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-32	Law Office of Wesley T. Umeda	CA	9/22/2017	Electronic	Business	Yes - Published #	215

On July 26, 2017, the forensic IT firm determined that there was no compromise of my computer network, but that my email account credentials were harvested on February 14, 2016, and my email account was accessed by an unauthorized person on July 3, 2017 and July 5, 2017. Such documents could include your: name, birth date, telephone number(s), address, Social Security number, employment (W-2) information, 1099 information, direct deposit bank account information including account number and routing information (if provided to me), and supporting records.

Attribution 1 Publication: NY AG's office Author:
Article Title: Law Office of Wesley T. Umeda
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-31	Tieks by Gavrieli	CA	8/17/2017	Electronic	Business	Yes - Published #	5,442

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Tieks by Gavrieli
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-29	Sunstar Americas.com	IL	7/20/2017	Electronic	Business	Yes - Published #	489

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Sunstar Americas.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-28	Success Partners	TX	7/1/2017	Electronic	Business	Yes - Published #	1,274

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Success Partners
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-27	Sole Society	CA	8/10/2017	Electronic	Business	Yes - Published #	2,829

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Sole Society
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-26	Shannon Restaurant	FL	8/10/2017	Electronic	Business	Yes - Published #	1,123

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Shannon Restaurant
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-25	Read-a-Thon Fundraising	TX	8/3/2017	Electronic	Business	Yes - Published #	1,595

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Read-a-Thon Fundraising
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-24	MSG Concessions	NY	8/17/2017	Electronic	Business	Yes - Published #	1,500

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: MSG Concessions
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-23	Holiday Valley Rest	NY	7/13/2017	Electronic	Business	Yes - Published #	824

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Holiday Valley Rest
Article URL: Per FOIL NY AG's office

Attribution 2 Publication: NY AG's office Author:
Article Title: Holiday Valley Rest
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-22	Halocigs	FL	7/1/2017	Electronic	Business	Yes - Published #	1,701

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Halocigs
Article URL: Per FOIL NY AG's office

Attribution 2 Publication: NY AG's office Author:
Article Title: Halocigs
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-21	Freshproduce.com	CO	7/27/2017	Electronic	Business	Yes - Published #	1,348

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Freshproduce.com
Article URL: Per FOIL NY AG's office

Attribution 2 Publication: NY AG's office Author:
Article Title: Freshproduce.com
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-20	Fairfield Mint, LLC	CT	8/10/2017	Electronic	Business	Yes - Published #	916

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Fairfield Mint, LLC
Article URL: Per FOIL NY AG's office

Attribution 2 Publication: NY AG's office Author:
Article Title: Fairfield Mint, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-19	Doubleline	TX	10/5/2017	Electronic	Business	Yes - Published #	1,637

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Doubleline
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-18	Direct Sports, Inc.	VA	7/1/2017	Electronic	Business	Yes - Published #	1,020

Per FOIL NY AG's office.

Attribution 1 Publication: NY AG's office Author:
Article Title: Direct Sports, Inc.
Article URL: Per FOIL NY AG's office

Attribution 2 Publication: NY AG's office Author:
Article Title: Direct Sports, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-17	COMBEX D2C	WI	7/13/2017	Electronic	Business	Yes - Published #	2,045

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: COMBEX D2C
Article URL: Per FOIL NY AG's office

Attribution 2 Publication: NY AG's office Author:
Article Title: COMBEX D2C
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-16	Catholic Answers	CA	7/20/2017	Electronic	Business	Yes - Published #	596

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: Catholic Answers
Article URL: Per FOIL NY AG's office

Attribution 2 Publication: NY AG's office Author:
Article Title: Catholic Answers
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-15	American Quilters Society	KY	8/31/2017	Electronic	Business	Yes - Published #	507

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: American Quilters Society
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-14	American Auto Parks	OK	9/28/2017	Electronic	Business	Yes - Published #	501

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: American Auto Parks
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-13	American Blue Ribbon Holdings	KY	7/20/2017	Electronic	Banking/Credit/Financial	Yes - Published #	5,770

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: American Blue Ribbon Holdings
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-12	All States AG Parts Inc.	WI	7/20/2017	Electronic	Banking/Credit/Financial	Yes - Published #	928

Per FOIL NY AG's office

Attribution 1 Publication: NY AG's office Author:
Article Title: All States AG Parts Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-11	Cislo Title Company	MI	12/29/2017	Electronic	Business	Yes - Published #	1,945

On May 18, 2017, our forensic investigator informed us that the email account had been compromised and an unauthorized individual may have had access to the informationstored in the account. The emails in the account contained loan-related documents as attachments, which may have contained your name, address, Social Security number, and driver's license information.

Attribution 1 Publication: NY AG's office Author:
Article Title: Cislo Title Company
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-10	Costco	WA	7/7/2017	Electronic	Banking/Credit/Financial	Yes - Published #	1,945

In mid-Jlme we discovered credit card skimming devices on the payment card temrinals at two cash registers in our Concordville Pennsylvania Costco warehouse. If your information was captured, the specific data involved would be the information on the magnetic stiipe of your payment card, including your name, payment card number, and card expiration date. If your payment card was a PIN debit card your PIN may have been captured as well.

Attribution 1 Publication: NYAG's office Author:
Article Title: Costco
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-09	Christi Benefits Group LLC	PA	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	1,200

On August 30, 2017, one of our employees was the target of a phishing scam. We believe that the unauthorized third party potentially accessed and acquired the following pieces of personal information about you: name; home address; email address; birthdate and Social Security
number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Christi Benefits Group LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-08	Capital One (9/19/2017)	VA	9/19/2017	Electronic	Banking/Credit/Financial	Yes - Published #	2,921

A former employee accessed your Bank account and passed on your information to an unauthorized third party. We have reversed the unauthorized transactions that we believe occurred to date, but please continue to keep an eye out for any additional unauthorized transactions and identity theft (including outside of Capital One®) because the person saw your account information, such as your name, address, email address, telephone number, Social Security Number, date of birth, telephone number and account number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Capital One (9/19/2017)
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-07	Canon Recruiting Group	CA	10/5/2017	Electronic	Business	Yes - Published #	Unknown

On August 28, 2017, we discovered that an employee was the subject of a phishing attack when they received an e-mail that appeared to be from an executive, requesting copies of employees' W-2 wage and tax statements. From our investigation, it appears that the documents contained your personal information, including your name, address, Social Security number, wages and tax information for 2016.

Attribution 1 Publication: NY AG's office Author:
Article Title: Canon Recruiting Group
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-06	Brace Industrial Group / Platinum Scaffolding Services	TX	7/1/2017	Electronic	Business	Yes - Published #	1,005

We recently learned that in late February 2017, a cybercriminal disguised an email to make it appear as if the email came from the president of the company, but in reality the email was meant to trick a Platinum workforce member into sending employee W-2s to the criminal. Unfortunately, the W-2s were sent in response, which allowed your 2016 W-2 statement to be released, including your Social Security number.

Attribution 1 Publication: NY AG's office Author:
Article Title: Brace Industrial Group / Plaatinum Scaffolding Services
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-05	Borden Duffel PC	TX	8/2/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 18, 2017, we discovered that your tax information stored within our server may have been accessed by an unknown, unauthorized third party. The investigation determined that your name, address, Social Security number and other tax information may have been accessed by an unauthorized third party.

Attribution 1 Publication: NY AG's office Author:
Article Title: Borden Duffel PC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-04	BLIIA, Inc. dba Oak Forest Montessori School	TN	7/25/2017	Electronic	Educational	Yes - Published #	415

On May 13, 2017 a member of the management team had her vehicle burglarized. On May 18, 2017, the manager realized that a portable USB drive that she uses for <<SchoolName>> business had been in her purse at the time of the crime and was therefore missing. The portable USB drive contained employee information and included your full name and Social Security number.

Attribution 1 Publication: NY AG's office Author:
Article Title: BLIIA, Inc. dba Oak Forest Montessori School
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-03	Archer Daniels Midland	NY	10/10/2017	Electronic	Banking/Credit/Financial	Yes - Published #	4,277

Unidentified malicious actors attempted to gain access to Asher Daniels Midland employees' email accounts in a scam known as a phishing attack. ADM completed its investigation of the incident on or around August 4, 2017 and concluded the scam potentially compromised the personal information of several individuals, including ADM employees, job applicants, and other third parties. The scam involved potential access to Social Security numbers, drivers' licenses or state identifiction card numbers, taxpayer identification numbers, credit and debit card information, banking information, passport numbers, medical information, health insurance information, and usernames and passwords for online accounts.

Attribution 1 Publication: NY AG's office Author:
Article Title: Archer Daniels Midland
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-02	Advanced Engine Management	CA	7/1/2017	Electronic	Business	Yes - Unknown #	

On March 22, 2017, Advanced Engine Management discovered that the email account of an Advanced Engine Management employee was compromised by an unauthorized individual. The email account may have contained the name, date of birth, address, Social Security Number, and health insurance information of the affected New York resident.

Attribution 1 Publication: NY AG's office Author:
Article Title: Advanced Engine Management
Article URL: Per FOIL request NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171229-01	ABC Carpet and Home	NY	10/10/2017	Electronic	Business	Yes - Published #	4,277

On August 9, 2017, ABC was notified that our online store, which is hosted and maintained by a vendor, may have been compromised. This transaction information may have included your name, address, telephone number, email address, credit card or debit card number, expiration date and security number.

Attribution 1 Publication: NY AG's office Author:
Article Title: ABC Carpet and Home
Article URL: Per FOIL request NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171228-03	BMO Harris Bank N.A.	IL	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	15,163

This personal information may have been accessible on PACER, an electronic public access service of the United States Federal Court System, which allows registered users to obtain information about a bankruptcy case. Depending on the document, the personal information may have been your: account number, date of birth, Social Security Number, Employer Identification Number, Driver's License or state-issued ID Number, Alien Registration number, Passport number, or the name of associated minor(s).

Attribution 1 Publication: NY AG's office Author:
Article Title: BMO Harris Bank N.A.
Article URL: Per FOIL Request

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171228-02	Horton Group, Inc.	IL	12/6/2017	Electronic	Business	Yes - Unknown #	Unknown

Horton immediately launched an investigation and ultimately learned that our company was the victim of email phishing attacks that prompted certain employees to provide their credentials to an unauthorized actor or actors. Our investigation has determined that the information present in the impacted email account includes your name and <<Data Elements>>.

Attribution 1 Publication: NH AG's office Author:
Article Title: Horton Group, Inc.
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/horton-group-20171206.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171228-01	Salinas Valley State Prison / CA Department of	CA	12/15/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

Confidential documents were inappropriately discarded and were discovered in an administration building trash by a staff member. These documents contained the names and social security numbers of staff employed at Salinas Valley State Prison as of January 15, 2016.

Attribution 1 Publication: CA AG's office Author:
Article Title: Salinas Valley State Prison / CA Department of Corrections and Rehabilitation
Article URL: https://oag.ca.gov/system/files/SVSP%20-%20Signed%20Privacy%20Breach%20Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-17	Choice Hotels International, Inc.	MD	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On April 26, 2017, we learned that certain employees responded to a phishing email sent on April 19, 2017 by providing their network credentials, which a third party then used to access your Workday account. We immediately launched an investigation and determined that your direct deposit information was changed and the unauthorized individual may have had access to your name, address, and Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Choice Hotels International, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285309.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-16	Muskingum County Library System	OH	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On Monday morning, March 13, 2017, we lost contact with one of our servers. We initially thought this was due to a recent update; however, further investigation pointed to a network intrusion from an unauthorized source. The information related to you that may have been subject to unauthorized access includes your name, Social Security number, date of birth, and bank account number related to your direct deposit.

Attribution 1 Publication: MD AG's office Author:
Article Title: Muskingum County Library System
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-282644.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-15	Allstate Insurance Company	IL	7/1/2017	Electronic	Business	Yes - Published #	358

On March 13, 2017 we became aware that a former Allstate agent may have used the names, addresses, and driver's license numbers of a Maryland resident to run a motor vehicle report, claim loss history report or credit report for an application for another individual. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Allstate Insurance Company
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-282414%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-14	**Maddaloni Nydick & Keenan, P.C.**	NJ	7/1/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On March 17, 2017, our forensic investigation firm confirmed that there was unauthorized access in our network between January 28, 2017 and February 10, 2017. The information related to you that may have been subject to unauthorized access includes your name, address and Social Security number.

Attribution 1 Publication: MD AG's office / ME AG's office Author:
Article Title: Maddaloni Nydick & Keenan, P.C.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-282647.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-13	**Delanco School District**	NJ	7/1/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

On January 13, 2017, Delanco discovered that a server holding certain employee and vendor data had been affected by a ransomware program that encrypted certain files on the server. The information related to your company that may have been subject to unauthorized access includes your company's name, address and tax identification number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Delanco School District
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-282655.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-12	**Manning & Napier**	NY	7/1/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On May 15th, an employee of Manning & Napier's Sales Department sent an email intended for your mother XXXXXXXXXXXX to an unrelated email address. The email included a beneficiary document that contained your name, address and social security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Manning & Napier
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-282654.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-11	**Ullico Inc.**	DC	7/1/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We are writing to notify you that unauthorized access to your personal information occurred on March 17, 2017. A closer review of those emails and attachments revealed that your personal information, specifically your name and SSN/Tax ID numbers were accessible in an attachment and may have been viewed by the unauthorized user.

Attribution 1 Publication: MD AG's office Author:
Article Title: Ullico Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285313.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-10	**Zillow Group, Inc.**	WA	7/1/2017	Electronic	Business	Yes - Published #	**1,912**

On May 9, 2017, a former Zillow Group employee inadvertently received a copy of your 2015 W-2 document due to a clerical error. The information involved includes name, address, and Social Security Number, as well as other wage and tax information in your 2015 W-2. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Zillow Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-282656.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-09	Red Lobster	FL	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 3, 2017, we discovered that the email account of one of our employees had become infected with a computer “virus,” which set up her account to automatically forward her incoming email messages to another unauthorized account.

Attribution 1 Publication: MD AG's office Author:
Article Title: Red Lobster
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-284800.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-08	Overseas Shipholding Group, Inc.	FL	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On April 18, 2017, we discovered that an OSG third party vendor, JiBe, LLC (“JiBe”), was the victim of a cyberattack. The information we believe that may have been accessed during this attack included your name, address, and Social Security Number.

Attribution 1 Publication: MD AG's office / ME AG's office Author:
Article Title: Overseas Shipholding Group, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285288%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-07	SingerLewak	CA	7/1/2017	Electronic	Business	Yes - Published #	262

SingerLewak discovered that an unknown individual or individuals had gained access to the email account of one of its employees. The information contained in the email account included names, addresses, dates of birth, Social Security numbers, and Financial Account numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: SingerLewak
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285290.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-06	M&T Bank	NY	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On Friday May 26, 2017 another customer brought to our attention that your personal checking account, savings account, and home equity line were accessible through his Web Banking login. Our records indicate that this other customer viewed a PDF version of your personal checking account statement and home equity statement on 5/26/2017 which include personal details such as your name, address, account balance, and account transactions.

Attribution 1 Publication: MD AG's office Author:
Article Title: M&T Bank
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285372.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-05	Onia / Acadaca, LLC	NY	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On April 11, 2017, Onia’s e-commerce service provider, Acadaca, LLC (“Acadaca”) discovered evidence of malicious code on all pages of Onia’s website. The personal and financial information of Onia customers was among the information accessed, including: (1) first and last name; (2) address; (3) email address; (4) telephone number; and (5) credit card number, expiration date, and CVV (the three digit security code found on the back side of your credit card).

Attribution 1 Publication: MD AG's office Author:
Article Title: Onia / Acadaca, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285368.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-03	**Holy Cross Home Care and Hospice**	MD	7/1/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

Our investigation of this incident confirmed that some of your private health information may have been on a computer drive that was stolen from one of our employees. The information may have included your name, address and birthdate, medical diagnosis, medical condition, and doctors name, insurance information, clinical notes and medications.

Attribution 1 Publication: MD AG's office Author:
Article Title: Holy Cross Home Care and Hospice
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285413%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171227-02	**Compassion Care Hospice Las Vegas, LLC**	NV	12/14/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,128**

Compassion Care Hospice Las Vegas, LLC NV Healthcare Provider 1128 12/14/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Compassion Care Hospice Las Vegas, 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
ITRC20171227-01	**Wager Evans Dental**	NV	12/27/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

A dental practice in Reno, NV has experienced a ransomware attack that prevented dental records and images from being accessed for five days. The malicious software was installed on one computer and one server used by the practice. The files encrypted by the ransomware contained sensitive information such as names, dates of birth, addresses, diagnoses, treatment plans, images, health insurance information, and Social Security numbers.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Access to Dental Records Lost for 5 Days Due to Ransomware
Article URL: https://www.hipaajournal.com/access-dental-records-lost-5-days-due-ransomware/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-14	**Union Bank & Trust (UBT)**	NE	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

In spite of our security measures, cyber attackers forced their way into our website in August or September of last year, inserting malware into the software supporting our website. This information would have included names, billing and shipping addresses, email addresses, credit card numbers, CVV ("Card Verification Value") numbers, credit card expiration dates, and website passwords.

Attribution 1 Publication: MD AG's office Author:
Article Title: Union Bank & Trust (UBT)
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285411%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-13	**Equity Resources, Inc.**	OH	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

The email address of the loan officer, Alex was compromised and emails were forwarded to an unknown person for about 6 hours until we discovered the issue. Private Information of yours including income documents you sent to Alex were forwarded to this unknown address.

Attribution 1 Publication: MD AG's office Author:
Article Title: Equity Resources, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285405.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-12	VW Credit Inc. (VCI)	OR	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

As set forth in the letter, VCI recently became aware that, due to a data processing error associated with a systems upgrade, between July 1, 2016 and May 23, 2017, in a small number of instances, certain VCI customers inadvertently gained access through the VCI online portal or written correspondence to the account information of another VCI customer with the same or similar name or address information. As a result of the data processing error described above, a VCI customer
may have had temporary access to some or all of the following information
related to another VCI customer's account: vehicle-type; account number;
vehicle identification number (VIN); name as entered on the account; full street address; phone numbers listed on the account; email address, if provided; total amount due on the account at the time viewed; AND MORE

Attribution 1
Publication: MD AG's office / NY AG's office Author:
Article Title: VW Credit Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286289.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-11	United Services Automobile Association (USAA)	TX	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 25, 2017, we discovered that, beginning approximately March 17, 2017, certain member personal information may have been accessible on a public website due to an administrative settings error at one of our vendors. The personal information of Maryland residents involved in the incident may have included first and last name, address,
telephone number, and bank account number.

Attribution 1
Publication: MD AG's office Author:
Article Title: United Services Automobile Association (USAA)
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-285418%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-10	Millennium Corporation	VA	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 26, 2017, Millennium received the attached notice from Paychex, Inc. (“Paychex”), a company that administers the “myStaffingPro” applicant tracking system through which Paychex provides services to Millennium. The notice states that “select client applicant data containing personally identifiable information in the form of social security numbers and/or driver’s license numbers on myStaffingPro’s e-sign website…could be accessed by various search engines without authentication.”

Attribution 1
Publication: MD AG's office Author:
Article Title: Millennium Corporation
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286194%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-09	National Treasury Employees Union	DC	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

I am writing pursuant to Maryland law to notify your office of an inadvertent disclosure of a document containing the name and Social Security Number (SSN) of 24 Maryland residents. The document was briefly accessible to 116 representatives from NTEU chapters and staff (NTEU representatives), who participated in union conducted
training related to the settlement of a night differential dispute with the IRS.

Attribution 1
Publication: Author:
Article Title: National Treasury Employees Union
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286193%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-08	Financial Edge	MD	7/1/2017	Electronic	Business	Yes - Published #	500

We are writing to inform you that we have learned of a breach of our computer systems by unauthorized individual(s) at our offices located in 2 E Rolling Crossroads Suite 251, Catonsville, MD 21228 between
possibly May 13, 2017 and May 18, 2017. On our systems, we maintain personal identifiable information (including, but not limited to, address and social security information) about our clients and their family members, various banking and account information, previous tax filings and related documentation and tax returns that are currently in the process of being prepared by us for the current year.

Attribution 1 Publication: MD AG's office Author:
Article Title: Financial Edge
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286237.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-07	John F Lewis PC	TX	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 30, our forensic investigation determined that an unauthorized individual accessed our system between April 19 and May 18, 2017. Information related to your tax filings may have been at risk, including your name, address, Social Security number, wage information and bank account information if you provided it to us.

Attribution 1 Publication: MD AG's office Author:
Article Title: John F Lewis PC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286199.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-06	HillPhoenix	GA	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 1, 2017, after HillPhoenix deposited outgoing mail into the mailbox outside of its facility in Conyers, GA, an SUV was observed driving up to the mailbox and removing the mail and driving away. Some of those mail items included personal identifying information, such as Social Security numbers, bank account numbers, and government file ID numbers related to support payments.

Attribution 1 Publication: MD AG's office Author:
Article Title: HillPhoenix
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286235.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-05	Lincoln Financial Group	PA	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

It was discovered that an insurance agent's personal information was compromised and used to gain unauthorized access to our website and view the agent's client information. This situation disclosed client name, address, date of birth, Social Security number and contract number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Lincoln Financial Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286205%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-04	NYU School of Medicine - Pediatric Surgery Associates	NY	12/15/2017	Paper Data	Medical/Healthcare	Yes - Published #	2,158

NYU School of Medicine - Pediatric Surgery Associates NY Healthcare Provider 2158 12/15/2017 Improper Disposal Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: NYU School of Medicine - Pediatric Surgery Associates
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=BD69D1C6514CE04ECCEAF2A522BF0F7D

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-03	Molina Healthcare	FL	12/21/2017	Electronic	Medical/Healthcare	Yes - Published #	1,380

Molina Healthcare FL Health Plan 1380 12/21/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Molina Healthcare
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=BD69D1C6514CE04ECCEAF2A522BF0F7D

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-02	SAY (Social Advocates for Youth)	CA	12/22/2017	Paper Data	Business	Yes - Published #	1,272

On October 27, 2017, SAY San Diego was notified by the County of San Diego Health & Human Services Agency ("HHSA") that a citizen had returned some paper files to their office that were found in a filing cabinet purchased from a salvage store. While we currently have no evidence that the clients' information was subject to any actual or attempted misuse, SAY San Diego confirmed that the files contained program participants' names, case numbers, dates and length of service received, locations of service, and provider names.

Attribution 1 Publication: databreaches.net / SAY press release Author:
Article Title: SAY San Diego Provides Notice Of Data Incident
Article URL: https://www.databreaches.net/say-san-diego-provides-notice-of-data-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171226-01	Colorado Mental Health Institute	CO	12/23/2017	Electronic	Government/Military	Yes - Published #	650

The Colorado Mental Health Institute at Pueblo is under the state's Department of Human Services. On December 22, it issued a notice following discovery of a phishing incident that potentially affected 650 patients.

Attribution 1 Publication: databreaches.net / healthcareitnews.co Author:
Article Title: Colorado Mental Health Institute at Pueblo notified 650 patients after phishing incident
Article URL: https://www.databreaches.net/colorado-mental-health-institute-at-pueblo-notified-650-patients-after-phishing-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171222-07	Houston Community College Foundation	TX	7/1/2017	Electronic	Educational	Yes - Unknown #	Unknown

On January 18, 2017, HCCF learned that GuideStar, an unaffiliated organization that provides an online, central repository of information on nonprofit organizations, disclosed on its website, www.guidestar.com, Houston Community College Foundation's IRS Forms 990 for calendar years 1997 to 1999, which inadvertently contained names and Social Security numbers of students that received scholarships from 1997 to 2000.

Attribution 1 Publication: MD AG's office Author:
Article Title: Houston Community College Foundation
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286210.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171222-06	Robert T. Bencivenga, CPA	NY	7/1/2017	Electronic	Business	Yes - Published #	538

The investigation determined that an unauthorized actor or actors gained
unauthorized access to Bencivenga's network and, consequently, to some personal information of certain Bencivenga clients and other individuals associated with those clients. The client information that was present on the affected systems may include the following categories
of information: name; address; Social Security number; wage/income information; date of birth, and, for some individuals, financial account information (such as bank account number and routing number) and/or driver's license number. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Robert T. Bencivenga, CPA
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286211.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171222-05	Life Time Fitness, Inc.	MN	7/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On April 3, 2017, we learned that some employees responded to a phishing email. The information that may have been accessed by the unauthorized person included your name, email address, home address, phone number, and the bank account information that you used for direct deposit of your paycheck.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Life Time Fitness, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286220.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171222-04	Reverse Mortgage Funding , LLC	NJ	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On May 23, 2017, RMF discovered that client information was contained in certain employee email accounts that it identified may have been accessed by an unauthorized party. While RMF is not aware of any misuse of client information, RMF has determined that certain clients' names, addresses, social security numbers and possibly driver's licenses and limited financial information may have been contained in the impacted email accounts.

Attribution 1 Publication: MD AG's office / ME AG's office Author:
Article Title: Reverse Mortgage Funding , LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286219.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171222-03	Bowman Business & Tax Services	TX	7/5/2017	Electronic	Business	Yes - Unknown #	Unknown

As noted in that letter, a number of events lead me to believe that information from our 2015 tax preparation may have been accessed by an unknown person or persons prior to the April 18, 2017 tax deadline. Such data could include sensitive personal information such as your name, address and Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Bowman Business & Tax Services
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286334.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171222-02	Federal Savings Bank	IL	7/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

A TFSB employee's laptop was stolen from the employee's personal car while it was parked off Bank property. The investigation revealed that the laptop contained certain personal information which may include the thirty Maryland residents' names and Social Security number or driver's
license number, or state identification number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Federal Savings Bank
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286336%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171222-01	Pharmacy Innovations	NY	12/12/2017	Electronic	Medical/Healthcare	Yes - Published #	1,205

Pharmacy Innovations NY Healthcare Provider 1205 12/12/2017 Hacking/IT Incident Network Server

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171221-08	Baker Tilly Virchow Krause, LLP	VA	7/7/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 9, 2017, Baker Tilly learned that one of its employees, as a result of a mistyped email address, inadvertently emailed some of its client's 2016 tax records to a third party emailaddress. As a result, one client's corporate tax records, which included a Maryland resident's name, address, and Social Security number, could have been viewed by an unauthorized person.

Attribution 1 Publication: MD AG's office Author:
Article Title: Baker Tilly Virchow Krause, LLP
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286353.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171221-07	**Health Hive, LLC**	CO	7/7/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On May 25,2017, a Health Hive employee's laptop was stolen. Shortly thereafter, Health Hive learned that the laptop contained unencrypted federal W-9 forms

Attribution 1 Publication: MD AG's office Author:
Article Title: Health Hive, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286348%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171221-06	**Delanco Township**	NJ	7/10/2017	Electronic	Government/Military	Yes - Unknown #	**Unknown**

On June 15, 2017, Delanco Township learned that an unauthorized individual was able to obtain compromised credentials for a single Township email account. While there is no indication that this unknown individual was able to access any other accounts or systems beyond this one email account, the investigation determined that some of the
Maryland resident's information was present in the email account, including name, address, and driver's license number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Delanco Township
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286399.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171221-05	**Real Estate Business Services, Inc.**	CA	7/10/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We recently learned that malicious code ("malware") uploaded by an unauthorized third party was present in payment processing software used for store.car.org. The data may have included the user's name, address, credit card number, credit card expiration date and, in some instances, credit card verification code (CVC code).

Attribution 1 Publication: MD AG's office Author:
Article Title: Real Estate Business Services, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286397.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171221-04	**LOGAN Community Resources, Inc.**	IN	7/11/2017	Electronic	Business	Yes - Unknown #	**Unknown**

The investigation determined that an unknown, unauthorized third-party gained access to several employees' email accounts, and could have viewed or accessed your personal information contained within these accounts. The potentially compromised information includes your name, address, date of birth, Social Security number and employee identification number. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: LOGAN Community Resources, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286412.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171221-03	**Best Buy Co., Inc.**	MN	7/11/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We have recently learned that certain U.S.-based, third-party call center agents (who have since been terminated) appear to have captured personal information of a limited number of Best Buy customers
without authorization.The personal information obtained by the call center agents may have included your name, postal address, email address, telephone number, and payment card information concerning the above-referenced payment card.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Best Buy Co., Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286408.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171221-02	Children's Hospital Los Angeles	CA	12/19/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On November 29, 2017, Children's Hospital Los Angeles ("CHLA") learned that your child's confidential health information was inadvertently transmitted to the wrong insurance payor. The insurance claim included the following information about your child: Name, Address, Medical Record Number, Date of Birth, Description of Services Provided, and Date of Service.

Attribution 1
Publication: CA AG's office Author:
Article Title: Children's Hospital Los Angeles
Article URL: https://oag.ca.gov/system/files/CHLA.Letter.Child__0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171221-01	Golden Optometric	CA	11/6/2017	Electronic	Medical/Healthcare	Yes - Published #	7,583

Early on the morning of November 6, 2017, the network server at Golden Optometric was infected with a variant of the "CrySiS" ransomware virus, which encrypted a limited number of files on its local drives. These documents generally included patient names, dates of birth, provider names, dates of service, purpose of the provider visit, blood pressure test results, diagnoses, medical record numbers, and health insurance subscriber identification numbers.

Attribution 1
Publication: CA AG's office / hhs.gov Author:
Article Title: Golden Optometric
Article URL: https://oag.ca.gov/system/files/Golden%20Optometric%20-%20Individual%20Notice%20%28Privileged%20%26%20Con

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171220-08	Geauga County	OH	12/20/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

In the course of the search, officials seized a number of Decatur's personal electronic devices, including a "drive" that contained a spreadsheet Decatur had prepared to comply with Affordable Care Act requirements. "The spreadsheet contained the personal information, including name, address, Social Security numbers and dates of birth of individual Geauga County employees and, in some instances, their spouses and children," Gliha said.

Attribution 1
Publication: geaugamapleleaf.com / databreaches.n Author:
Article Title: Geauga County
Article URL: https://www.geaugamapleleaf.com/news/county-employees-notified-of-data-security-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171220-07	Chilton Medical Center	NJ	12/20/2017	Electronic	Medical/Healthcare	Yes - Published #	4,600

On October 31, 2017, we learned that an employee had removed a computer hard drive from the hospital in violation of Chilton Medical Center policy and sold it on the internet earlier that month. Our investigation determined that the hard drive contained patient information, and may have included patients' names, dates of birth, addresses, medical record numbers, allergies, and medications the patient may have received at Chilton Medical Center.

Attribution 1
Publication: company website / hhs.gov Author:
Article Title: Chilton Medical Center
Article URL: http://www.chiltonhealth.org/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171220-06	NYU Langone Health System	NY	12/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	2,000

NYU Langone Health System discovered a binder containing a log of presurgical insurance authorizations was accidentally recycled by a cleaning company in October. Information in the binder included names, birth dates, dates of service, current procedural terminology code, diagnosis codes, insurer names, and insurance ID numbers.

Attribution 1
Publication: hipaajournal.com Author:
Article Title: NYU Langone Health System
Article URL: https://www.hipaajournal.com/healthcare-providers-improper-disposal-patient-data/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171220-05	**MidMichigan Medical Center**	MI	12/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	**1,900**

On the evening of November 18, a MMC cardiologist removed patient files from the Alpena cardiology office without authorization. Approximately 1,900 patients have been notified of the potential breach, which may have included names along with addresses, Social Security numbers, and clinical data.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 1,900 MidMichigan Medical Center Patients Notified After Documents Found in the Street
Article URL: https://www.hipaajournal.com/1900-midmichigan-medical-center-patients-notified-documents-street/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171220-04	**TIO Networks / Pay**	CA	12/4/2017	Electronic	Business	Yes - Published #	**1,600,000**

PayPal Holdings on Friday acknowledged that a data breach at recently acquired payments processor TIO Networks compromised the personally identifiable information of roughly 1.6 million customers. Justin Higgs, a senior manager of corporate communications at PayPal, later clarified to SC Media via email that “potential information that was compromised includes data such as payment card information or bank account information, usernames and passwords for online accounts, and Social Security.”

Attribution 1 Publication: scmagazine.com Author:
Article Title: PayPal shelled out $238 million for company that may have had 1.6 million customers breached
Article URL: https://www.scmagazine.com/data-breach-at-paypals-tio-networks-unit-affects-16-million-customers/article/711484/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171220-03	**Metropolitan Life Insurance Company**	NY	11/9/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On November 9, 2017, a group life enrollment report was sent by a MetLife associate to two associates that are affiliated with a group life customer with which you are not employed. The inadvertently disclosed email attachment contained your name, Social Security number and group life coverage election amounts.

Attribution 1 Publication: CA AG's office Author:
Article Title: Metropolitan Life Insurance Company
Article URL: https://oag.ca.gov/system/files/CA%20Notification%20Letter%20%2810721%29_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171220-02	**College of the Siskiyous**	CA	12/15/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

On December 13, 2017, Siskiyou Joint Community College District received email notice that First Capitol Consulting, Inc. had inadvertently disclosed District sensitive information to another client, Ramapo Communication Corporation. The data included sensitive employer and employee information including employer identification numbers, social security numbers, addresses, dates of birth, payroll information, and job positions.

Attribution 1 Publication: CA AG's office Author:
Article Title: College of the Siskiyous
Article URL: https://oag.ca.gov/system/files/COSDataBreach12-13-17_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171220-01	**Pinterest**	CA	11/24/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Your email address and password may have been obtained by hackers through a breach of other websites, and that information may have been used to log in to your Pinterest account and send spam.

Attribution 1 Publication: CA AG's office Author:
Article Title: Pinterest
Article URL: https://oag.ca.gov/system/files/2017.12.08%20Pinterest%20User%20Notice_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-12	Farmers and Merchants Trust Company of Chambersburg	PA	7/13/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On June 1, 2017, we learned that an unauthorized individual may have gained access to an employee's email account. We conducted a thorough review of the employee'semail account and determined that it may have contained some personal information, including your name, date of birth, bank account number, and Social Security number.

Attribution 1 Publication: MD AG's office / NY Ag's office Author:
Article Title: Farmers and Merchants Trust Company of Chambersburg
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286458.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-11	Sunbelt Rentals, Inc.	SC	7/17/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 12, 2017, Sunbelt was the victim of a "spear-phishing" email campaign that used a spoofed email made to appear as though it came from Sunbelt's Senior Vice President of Information Technology. By accessing Workday, it is possible, but not yet determined, that the bad actors may have viewed sensitive personal information, including the employees' name, address, e-mail address, company user name and password, social security number, payroll information, and limited information regarding any dependents and beneficiaries that are currently listed in Workday, but not the dependents' and beneficiaries' social security numbers.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Sunbelt Rentals, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286473.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-10	Rose Harrison & Gilreath, P.C.	NC	7/17/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 12, 2017, we discovered that one of our internal email accounts had been compromised as a result of a phishing scam. We have conducted an investigation and determined that an email containing your social security number and bank account information sent to this email account was inadvertently redirected to an unknown third party.

Attribution 1 Publication: MD AG's office Author:
Article Title: Rose Harrison & Gilreath, P.C.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286472.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-09	Stuart, Edelstein, Linderman & Co., Inc.	NY	7/18/2017	Electronic	Business	Yes - Unknown #	Unknown

Recently several New York accounting firms, including ours, fell victim to a data compromise. Immediate steps were taken to protect your information from further risk. Data that may have been accessed include: name, address, date-of-birth, social security number and tax information, in addition to the information of anyone else included on your filing.

Attribution 1 Publication: MD AG's office Author:
Article Title: Stuart, Edelstein, Linderman & Co., Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286509%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-08	Ameriprise Financial Services, Inc.	MN	7/13/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On February 10, 2017, a copy of an advisor's client list was uploaded to their personal email account as part of their transition to Ameriprise Financial. The client list included personal information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Ameriprise Financial Services, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286444.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-07	Michael Friedland, LTD	IL	7/12/2017	Electronic	Business	Yes - Published #	622

On or about June 12, 2017, the firm became aware that it may have been a victim of a cyber-attack by which an unknown third party was able to access its computer network and some of its clients' personal information. As a result, some of the firm's client's personal information may have been exposed to others, including their first and last names, home addresses, social security numbers, and 2015 and 2016 tax retum information, including compensation data. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Michael Friedland, LTD
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286424.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-06	Hotel Preston / Aspen Tennessee	TN	7/14/2017	Electronic	Business	Yes - Published #	269

The investigation identified signs that an unauthorized program was installed on one of the payment terminals at our front-desk designed to copy data as it was input into the terminal. The data copied by the program included payment card data – including cardholder name, payment card account number, card expiration date, and internal verification code – of certain guests who used a payment card at this one terminal during the period from July 12, 2016 to August 3, 2016.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Hotel Preston
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286468.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-05	Chizner & Company CPA's LLC	NY	7/21/2017	Electronic	Business	Yes - Published #	208

Although our investigation is ongoing, it appears that unauthorized individuals may have gained access to Chizner's tax account management and filing system, potentially compromising tax account related information including your and any listed dependents' Social Security numbers, addresses, tax refund financial account
information, and other information associated with your tax return. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Chizner & Company CPA's LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286525.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-04	Katz Abosch, Windesheim, Gershman & Freedman, PA	MD	7/24/2017	Electronic	Business	Yes - Unknown #	Unknown

After a member of our organization opened a malicious link in an email,
we received reports that spam messages were sent to that employee's contacts. The investigation determined that the compromised email account contained your name and Social Security number, and that this information was potentially obtained by an unauthorized third-party

Attribution 1 Publication: MD AG's office Author:
Article Title: Katz Abosch, Windesheim, Gershman & Freedman, PA
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286529.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-03	GlassRoom Advisors, LLC	VA	7/26/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

I am writing on behalf of my client, GlassRoom Advisors LLC ("GlassRoom"), to notify your office that last month, GlassRoom learned someone apparently accessed the email account of one of its employees. The unauthorized individual may have obtained access to subscription documents containing name, address, social security numbers or tax IDs, and bank account information for two (2) Maryland residents/entities.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: GlassRoom Advisors, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286538%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-02	**Alteryx**	CA	12/19/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Information on more than 120 million American households was sitting in a massive database found left exposed on the web earlier this month, Forbes has been told. It included an extraordinary range of personal details on residents, including addresses, ethnicity, interests and hobbies, income, right down to what kind of mortgage the house was under and how many children lived at the property.

Attribution 1 Publication: Forbes Author:
Article Title: 120 Million American Households Exposed In 'Massive' ConsumerView Database Leak
Article URL: National Cyber Security Alliance

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171219-01	**AmediStaf, LLC dba The Right Solutions / Conexus**	AR	12/15/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

On October 31, 2017, TRS discovered that a web application directory (the " Directory") containing certain personal information of a limited number of TRS nurse clients was potentially accessible from the Internet from September 5, 2015 to November 2, 2017. configured. Although our investigation is ongoing, we believe that the Directory contained a profile containing certain of your personal information, possibly including your name, date of birth, driver's license number, and/or Social Security number.

Attribution 1 Publication: MT AG's office Author:
Article Title: AmediStaf, LLC dba The Right Solutions
Article URL: https://dojmt.gov/wp-content/uploads/TRS-Healthcare.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-16	**City of Fond du Lac**	WI	12/16/2017	Electronic	Government/Military	Yes - Unknown #	**Unknown**

The City of Fond du Lac says people who made payments using the online system between August and October of this year may have had their credit card numbers taken.

Attribution 1 Publication: kfiz.com Author:
Article Title: City of Fond du Lac Warns of Possible Credit Card Info Breach
Article URL: http://www.kfiz.com/local-news/city-of-fond-du-lac-warns-of-possible-credit-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-15	**Shamrock Financial Corporation**	RI	12/8/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

At some point prior to August 2, 2017, as a result of a sophisticated social engineering intrusion, a third party gained access to Shamrock's systems in an attempt to redirect wiring instructions. Based on the circumstances of the intrusion, there is a possibility that the third party had access to customer loan applications, which include name, address, date of birth, Social Security number and financial information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Shamrock Financial Corporation
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/shamrock-financial-20171208.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-14	**IH Mississippi Valley Credit Union**	IL	12/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

On October 2, 2017, IHMVCU learned that a credit union employee was the victim of an email phishing scam. The information that could have been affected includes the following categories of information: Name, address, Social Security number, and/or member account number. IHMVCU has no evidence of the actual or attempted misuse of this information.

Attribution 1 Publication: NH AG's office Author:
Article Title: IH Mississippi Valley Credit Union
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/ih-mississippi-20171201.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-13	MFTStamps.com / Inspired by… / Gorilla GEMS, Inc.	FL	12/7/2017	Electronic	Business	Yes - Unknown #	Unknown

(MFTStamps.com / Inspired by…) We have reason to believe that a Gorilla administrative username and password, and transitively the electronic order and payment systems, were compromised for a period of time, revealing customer information. A malicious software was implanted by an unknown overseas source and it appears that customer order information including customer names, billing and shipping addresses, credit card information, and contact information, used in connection with orders placed from June 22, 2017, through the morning of August 15, 2017, may have been compromised.

Attribution 1 Publication: NH AG's office / MT AG's office Author:
Article Title: MFTStamps.com
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/inspired-by-20171207.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-12	Hayden, Narey & Persich	CA	12/6/2017	Electronic	Business	Yes - Unknown #	Unknown

While filing returns on extension, we encountered suspicious electronic activity in our tax program with some federal tax returns inexplicably rejected. As a partner, shareholder or beneficiary of a partnership, company, or trust we performed work for, the information may have included your: first and last name, address, Social Security number, and the losses and gains earned from that entity.

Attribution 1 Publication: NH AG's office Author:
Article Title: Hayden, Narey & Persich
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/hayden-20171204.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-11	Connecticut Parent Advocacy Center	CT	7/26/2017	Paper Data	Business	Yes - Unknown #	Unknown

On or about the morning of Tuesday June 20 our employees arrived at work and noticed two file cabinet drawers were open. Unknown details.

Attribution 1 Publication: NH AG's office Author:
Article Title: Connecticut Parent Advocacy Center
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/connecticut-parent-advocacy-20170726.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-10	Bennington-Rutland Supervisory Union	VT	12/6/2017	Electronic	Educational	Yes - Unknown #	Unknown

On July 6, 2017, we discovered our computer system had been infected with a virus that prohibited our access to our files. While there is a potential that this third party gained access to your personal information, we are currently unaware of any attempted or actual access or misuse of your information has occurred. <<Data Element Paragraph>>

Attribution 1 Publication: NH AG's office Author:
Article Title: Bennington-Rutland Supervisory Union
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/bennington-rutland-20171206.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-09	Louisiana State University	LA	12/15/2017	Electronic	Educational	Yes - Published #	5,500

LSU is mailing letters to approximately 5,500 individuals whose information may have been contained on a university-owned laptop that was recently stolen from an LSU employee. That investigation determined the laptop may have contained individuals' full names, dates of birth, Social Security numbers and/or driver's license numbers. The laptop may also have contained the names and credit card information for a very small number of individuals.

Attribution 1 Publication: ktbs.com Author:
Article Title: LSU issues notifications regarding stolen laptop
Article URL: https://www.ktbs.com/news/lsu-issues-notifications-regarding-stolen-laptop/article_22377450-e1e9-11e7-858b-8f41eb0

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-08	University of Alabama at Birmingham	AL	11/27/2017	Electronic	Medical/Healthcare	Yes - Published #	652

University of Alabama at Birmingham AL Healthcare Provider 652 11/27/2017 Loss Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: University of Alabama at Birmingham
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=83E5114D9F13AD1C39868D2D64631904

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-07	Golden Rule Insurance Company	IN	12/4/2017	Electronic	Medical/Healthcare	Yes - Published #	9,305

Golden Rule Insurance Company IN Health Plan 9305 12/04/2017 Unauthorized Access/Disclosure Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Golden Rule Insurance Company
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=83E5114D9F13AD1C39868D2D64631904

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-06	Austin Manual Therapy Associates	TX	12/6/2017	Electronic	Medical/Healthcare	Yes - Published #	1,750

On October 9, 2017, we learned that a criminal attacker accessed our system without authorization. Based on the information stored on that computer and shared file system, the attacker may have been able to obtain some patient names and, in some circumstances one or more of the following types of information: addresses, phone numbers, occupations, dates of birth, insurance policy information, insurance coverage and eligibility information, charge amounts, dates of service, driver's license information, diagnosis, health screening information, referring physician information, and full or partial social security numbers.

Attribution 1 Publication: hhs.gov / databreaches.net / AMTA notifi Author:
Article Title: Austin Manual Therapy notifies 1,750 patients of data breach
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=83E5114D9F13AD1C39868D2D64631904

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-05	Columbus Surgery Center	NE	12/7/2017	Electronic	Medical/Healthcare	Yes - Published #	7,221

The ransomware attack occurred on October 7, 2017 and saw a wide range of files on some servers being encrypted by the ransomware. The investigation did not uncover evidence to suggest any patient health information was stolen, but data access could not be ruled out with a high degree of confidence.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Columbus Surgery Center
Article URL: https://www.hipaajournal.com/almost-10000-patients-impacted-nebraska-ransomware-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-04	Mount Carmel Health System	OH	12/8/2017	Electronic	Medical/Healthcare	Yes - Published #	836

Mount Carmel Health System OH Healthcare Provider 836 12/08/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Mount Carmel Health System
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=83E5114D9F13AD1C39868D2D64631904

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-03	Central Iowa Hospital Corporation / dba Blank	IA	12/8/2017	Electronic	Medical/Healthcare	Yes - Published #	557

Central Iowa Hospital Corporation d/b/a Blank Children's Hospital IA Healthcare Provider 557 12/08/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Central Iowa Hospital Corporation / dba Blank Children's Hospital
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=83E5114D9F13AD1C39868D2D64631904

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-02	University of South Florida / USF Health Care	FL	12/11/2017	Paper Data	Medical/Healthcare	Yes - Published #	1,279

University of South Florida, USF Health Care FL Healthcare Provider 1279 12/11/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: University of South Florida / USF Health Care
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=83E5114D9F13AD1C39868D2D64631904

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171218-01	California Secretary of State	CA	12/15/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

Kromtech Security's Bob Diachenko that earlier this month Kromtech came across an database named cool_db containing 19.2 million voter records gathered in two collections that was fully unprotected and thus open for anyone to view. One batch contained voter registration data for a local district and the other the millions of records.

Attribution 1 Publication: scmagazine.com Author:
Article Title: California Secretary of State
Article URL: https://www.scmagazine.com/millions-of-california-voter-records-exposed-in-unprotected-mongodb/article/719028/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171215-03	Washington Health System Greene	PA	12/15/2017	Electronic	Medical/Healthcare	Yes - Published #	4,145

A portable hard drive used with a bone densitometry machine in the Radiology department was discovered to be missing on October 11, 2017. While it is possible that the hard drive may have been misplaced, a search of the hospital did not uncover the device, and the missing device has been reported to the Pennsylvania State Police Department as a potential theft. The information stored on the device was limited to names, height, weight, race, and gender, while some patients also had details of health issues, the name of their prescribing physician, and medical record numbers stored on the device.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Washington Health System Greene Discovers Hard Drive Missing
Article URL: https://www.hipaajournal.com/texas-pennsylvania-data-breaches-exposed-5000-patients-phi/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171215-02	Board of Pensions of the Presbyterian Church (USA)	PA	12/11/2017	Electronic	Business	Yes - Unknown #	Unknown

On December 1, 2017, The Board of Pensions ofthe Presbyterian Church (U.S.A.) learned that unauthorized Benefits Connect logons had been established for certain pensioners who had not previously registered for Benefits Connect, and that contact and bank account information for those pensioners had been altered without pensioner authorization.

Attribution 1 Publication: MT AG's office Author:
Article Title: Board of Pensions of the Presbyterian Church (USA)
Article URL: https://dojmt.gov/wp-content/uploads/The-Board-of-Pensions-of-the-Presbyterian-Church-U.S.A.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171215-01	Farm Bureau Financial Services	IA	12/8/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On November 27, 2017, our investigation of a suspected email phishing incident concluded. This includes information such as your name, address, Social Security number, and, for some individuals, may also have included your date of birth, driver's license number, financial account number, signature, or health-related information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171214-01	Bank of the West	CA	12/5/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On October 5, 2017 Bank of the West was informed by Dallas police that an individual had been arrested and was in possession of documents related to Bank of the West loan accounts. The loan documents contain your personal information, such as your name, address, phone number, Social Security number, driver's license number, and date of birth.

Attribution 1 Publication: MT AG's office / NH AG's office Author:
Article Title: Bank of the West
Article URL: https://dojmt.gov/wp-content/uploads/Bank-of-the-West.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171213-07	Taconic Capital Advisors, LP	NY	7/28/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On July 21, 2017, State Street, the fund administrator for Taconic, notified Taconic that it had inadvertently sent some data related to Taconic investors to a third party.

Attribution 1 Publication: MD AG's office Author:
Article Title: Taconic Capital Advisors, LP
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286544.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171213-06	U.S. Residential Group, LLC	TX	8/2/2017	Electronic	Business	Yes - Unknown #	Unknown

A U.S. Residential employee was recently targeted by a phishing scam and inadvertently shared login information for their company email account. Some of the files and documents stored in the email account contained certain information about some current and former U.S. Residential employees and/or their dependents, including name, social security number, business financial account numbers, driver's license or government identification number, and in some cases medical or health insurance information and identifiers.

Attribution 1 Publication: MD AG's office Author:
Article Title: U.S. Residential Group, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286792.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171213-05	Botwinick & Co., LLC	NJ	8/4/2017	Electronic	Business	Yes - Unknown #	Unknown

Although the investigation has not identified evidence of compromise to clients' information, it is possible that personally identifiable information ("PII"), including names, Social Security numbers and tax information may have viewed or accessed by an unknown and unauthorized third-party.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Botwinick & Co., LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286552.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171213-04	Stoy, Malone & Company, P.C.	MD	8/7/2017	Electronic	Business	Yes - Unknown #	Unknown

On July 6, 2017, Stay learned that an unauthorized third party gained access to an employee's email account. The investigation determined that emails or attachments in the account contained the name, address, and Social Security number of 38 Maryland residents.

Attribution 1 Publication: MD AG's office Author:
Article Title: Stoy, Malone & Company, P.C.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286558.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171213-03	**Midland Memorial Hospital District dba Midland**	TX	12/12/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,160**

The hospital became aware on Oct. 13 that an unauthorized third party may have obtained access to an employee's e-mail account on or about Oct. 10. During the relevant period, certain patient information was contained in a limited number of e-mails stored in the employee's account, including patients' first and last names, account numbers/medical record unit numbers and other information relating to radiology procedure(s) performed at the hospital in August and September.

Attribution 1 Publication: mrt.com / hipaajournal.com / hhs.com Author:
Article Title: MMH announces 'data security incident' involving patient information
Article URL: http://www.mrt.com/news/article/MMH-announces-data-security-incident-12425589.php

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171213-02	**Franciscan Physician Network of IL / Specialty**	IL	12/13/2017	Paper Data	Medical/Healthcare	Yes - Published #	**22,000**

On November 21, 2017, it was confirmed that a limited number of boxes that contained 22,000 patient payment records could not be located in a shared record storage facility located in Chicago Heights, Illinois. The information included patient name, address, payment date, payment amount, payment method, office location and the last four digits of patient credit card numbers.

Attribution 1 Publication: databreaches.net / hipaajournal.com Author:
Article Title: Franciscan Physician Network of IL / Specialty Physicians of IL
Article URL: https://www.databreaches.net/franciscan-physician-network-of-illinois-and-specialty-physicians-of-illinois-notify-patie

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171213-01	**U-Haul Co. of California / Solo Tire**	CA	12/11/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Findings from our investigation suggest that one computer workstation at this dealership had been infected with malware designed to target payment card information, but which may have also accessed other rental information.This information may have included your name, address, phone number, email address, driver's license number, birth date, and payment card number and expiration date.

Attribution 1 Publication: CA AG's office / MT AG's office Author:
Article Title: U-Haul Co. of California / Solo Tire
Article URL: https://oag.ca.gov/system/files/CA.UHaulNotification-withcard.12.11.2017_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171212-01	**WEI Mortgage LLC**	VA	12/8/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

On or around September 20, 2017, WEI Mortgage LLC ("WEI Mortgage") received reports of unusual activity in an employee's email account. Our investigation determined the information present in the impacted email account includes your Social Security number, address, and name.

Attribution 1 Publication: CA AG's office / NH AG's office / OR AG Author:
Article Title: WEI Mortgage LLC
Article URL: https://oag.ca.gov/system/files/WEI%20Mortgage%20-%20Notice%20only%200_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171211-08	**Eye Physicians, P.S.**	NE	12/7/2017	Electronic	Medical/Healthcare	Yes - Published #	**2,620**

On October 7, 2017, we were the target of a ransomware attack that encrypted files maintained on some of our servers. In order to continue to see patients, we immediately restored our servers from a recent backup. Although the investigation did not identify any evidence of access to your information, we could not rule out the possibility that your personal information, including your name, date of birth, and ophthalmic imagery may be at risk. No Social Security numbers, financial transactions or payment information were involved in this incident.

Attribution 1 Publication: MT AG's office / hipaajournal.com Author:
Article Title: Eye Physicians
Article URL: https://dojmt.gov/wp-content/uploads/Eye-Physicians.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171211-07	IdeaStream	OH	11/30/2017	Electronic	Business	Yes - Unknown #	Unknown

On November 1, 2017, the company that manages our website informed us that they had detected malicious code on our site while running a security scan. The information potentially disclosed includes customer names, e-mail addresses, mailing addresses, and payment information, including credit card information. No social security numbers were disclosed.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171211-06	Glen Falls Hospital	NY	12/8/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

The names and Social Security numbers of Glens Falls Hospital employees who had not received flu shots were released in an internal email to staff, according to a letter from management obtained by The Post-Star. Hospital officials said that the management group received an email from the Center for Occupational Health, regarding the influenza immunization status of employees. A report was attached to the email, which included employee names and their Social Security numbers, according to a copy of the Dec. 1 letter to staff obtained by The Post-Star.

Attribution 1 Publication: poststar.com Author:
Article Title: Glens Falls Hospital workers' Social Security numbers released in internal email
Article URL: http://poststar.com/news/local/glens-falls-hospital-workers-social-security-numbers-released-in-internal/article_02a66

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171211-05	Clarion University	PA	12/7/2017	Electronic	Educational	Yes - Published #	408

Clarion University was notified of an email compromise that occurred because of a criminal phishing scam that compromised two email accounts in the registrar's office. "The email compromise potentially exposed Social Security and/or driver's license numbers belonging to 408 students.

Attribution 1 Publication: explorerclarion.com Author:
Article Title: Clarion University Email Compromised, Investigation Underway
Article URL: http://www.exploreclarion.com/2017/12/07/clarion-university-email-compromised-investigation-underway/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171211-04	Village of Nashotah	WI	12/8/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

The village recently paid an unidentified hacker a $2,000 ransom to decrypt its computer system after a hack in late November that left some residents' personal information exposed. He said the only information that was exposed during the breach were citizens' names and driver's license numbers, and possibly their addresses.

Attribution 1 Publication: jsonline.com / WI AG's office Author:
Article Title: Village of Nashotah
Article URL: https://www.jsonline.com/story/communities/lake-country/news/nashotah/2017/12/08/after-computer-hack-nashotah-p

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171211-03	National Capital Poison Center	DC	12/8/2017	Electronic	Business	Yes - Unknown #	Unknown

In October 2017, NCPC discovered it had experienced a ransomware infection. The database server contains one or more of the following types of information captured during call center calls, if the information was provided: caller name, name of person possibly exposed to a poisonous substance and date of birth, address and telephone number, information about the exposure and clinical course, recommendations provided to the caller, caller's email address, and if applicable, treating facility name and medical record number.

Attribution 1 Publication: CA AG's office / OR AG's office Author:
Article Title: National Capital Poison Center
Article URL: https://oag.ca.gov/system/files/NCPC%20Exhibit%201%20to%20CA%20Regulator%20Notice_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171211-02	CCRM Minneapolis, P.C.	MN	12/5/2017	Electronic	Medical/Healthcare	Yes - Published #	3,280

CCRM Minneapolis, P.C. MN Healthcare Provider 3280 12/01/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: CCRM Minneapolis, P.C.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=01057816904528553A6563B48D873696

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171211-01	Oklahoma Department of Human Services	OK	12/5/2017	Electronic	Government/Military	Yes - Published #	47,000

An unauthorized user accessed a state assessment computer at Carl Albert State College in Poteau, Oklahoma, in April 2016. The server contained the names, addresses, dates of birth and Social Security numbers of both current and former DHS Temporary Assistance for Needy Families clients.

Attribution 1 Publication: hhs.gov / healthcarenews.com Author:
Article Title: Oklahoma health department alerts 47,000 clients about data breach for the 2nd time
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=01057816904528553A6563B48D873696

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-12	Texas Department of Agriculture	TX	12/7/2017	Electronic	Government/Military	Yes - Published #	700

According to the agency's security notice on its website, an employee's state-issued laptop was attacked by a type of malicious software called "ransomware," which threatens to publish data unless a ransom is paid. Officials said that information could include names, home addresses, birth dates, phone numbers and Social Security numbers of students and their families.

Attribution 1 Publication: dentonrc.com Author:
Article Title: Five Denton County schools impacted by state agency data breach
Article URL: http://www.dentonrc.com/news/news/2017/12/07/five-denton-county-schools-impacted-state-agency-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-11	This Works Products, Ltd.	US	11/30/2017	Electronic	Business	Yes - Unknown #	Unknown

On October 19, 2017, we became aware of suspicious activity on our website network leading us to believe an unlawful intrusion had occurred. This includes your name, e-mail address, home address, shipping address, phone number and payment card details (including credit card account number, expiration month and year and Card Verification Value ("CVV") code) used for the transaction.

Attribution 1 Publication: NH AG's office Author:
Article Title: This Works Products, Ltd.
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/this-works-products-20171130.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-10	Lincoln Financial Group	PA	11/29/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Lincoln recently discovered that a home office employee was the victim of a phishing attack which resulted in a third party gaining limited access to the employee's email account for a period of time between October 19 and 20, 2017. We have determined that this unauthorized access may have exposed the personal information, consisting of name and Social Security number of 6 residents.

Attribution 1 Publication: NH AG's office Author:
Article Title: Lincoln Financial Group
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/lincoln-financial-20171129.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-09	**Image Group**	OH	11/29/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On approximately November 17, 2017, The Image Group discovered and promptly resolved a temporary security vulnerability on our eCommerce platform. During this period of time, the following information related to certain The Image Group customers may have been vulnerable to unauthorized access: name, email address, delivery /billing address, credit card type, and credit card number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Image Group
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/image-group-20171128.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-08	**UNC Health Care / Dermatology & Skin Care**	NC	12/8/2017	Electronic	Medical/Healthcare	Yes - Published #	**24,000**

UNC said Friday that personal patient information was contained on a hard drive of a laptop computer that was stolen from UNC Dermatology & Skin Cancer Center in October. The laptop's patient database contains patient names, addresses, phone numbers, employment status, employer names, birth dates and Social Security numbers.

Attribution 1 Publication: newsobserver.com Author:
Article Title: 24,000 UNC Health Care patients affected by potential security breach
Article URL: http://www.newsobserver.com/news/business/article188757969.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-07	**Sutter Valley Medical Foundation dba Sutter**	CA	11/22/2017	Paper Data	Medical/Healthcare	Yes - Published #	**1,303**

Sutter Valley Medical Foundation d/b/a Sutter Medical Foundation CA Healthcare Provider 1303 11/22/2017 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Sutter Valley Medical Foundation dba Sutter Medical Foundation
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-06	**Bronson Healthcare Group**	MI	12/5/2017	Electronic	Medical/Healthcare	Yes - Published #	**8,256**

Bronson Healthcare Group MI Healthcare Provider 8256 12/05/2017 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Bronson Healthcare 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
ITRC20171208-05	**Hackensack Sleep and Pulmonary Center**	NJ	12/8/2017	Electronic	Medical/Healthcare	Yes - Published #	**16,474**

The New Jersey-based Hackensack Sleep and Pulmonary Center, specialists in sleep disorders and pulmonary conditions and diseases, has experienced a ransomware attack that resulted in the protected health information of certain patients being encrypted. The types of information encrypted included diagnoses, notes, procedures, and patient reports, along with names, addresses, Social Security numbers, dates of birth, insurance information, credit card numbers, and account information.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: New Jersey Sleep Medicine Specialists Experience Ransomware Attack
Article URL: https://www.hipaajournal.com/new-jersey-sleep-medicine-specialists-experience-ransomware-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-04	Sinai Health System	IL	12/8/2017	Electronic	Medical/Healthcare	Yes - Published #	11,350

The email accounts of two employees of Chicago's Sinai Health System have been compromised in a recent phishing attack. No evidence has been uncovered to suggest any financial information was accessed, although an analysis of the email accounts revealed a range of protected health information of 11,350 patients was contained in the email accounts and could potentially have been viewed.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: 11,350 Sinai Health System Patients Potentially Impacted by Phishing Attack
Article URL: https://www.hipaajournal.com/11350-sinai-health-system-phishing-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-03	Pulmonary Specialists of Louisville	KY	11/28/2017	Electronic	Medical/Healthcare	Yes - Published #	32,000

On September 26, 2017, we identified possible unauthorized access to our electronic health record (EHR) system. The investigation determined that an unknown, unauthorized third party may have gained access to our practice's EHR and could have viewed or accessed your electronically stored information, including your name, address, phone
number, date of birth, Social Security number, health insurance information and medical records.

Attribution 1 Publication: MT AG's office / NH AG's office / hhs.go Author:
Article Title: Pulmonary Specialists of Louisville
Article URL: https://dojmt.gov/wp-content/uploads/Pulmonary-Specialists-of-Louisville.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-02	Amazing Grass	CA	11/30/2017	Electronic	Business	Yes - Unknown #	Unknown

Based on the forensic firm's investigation, we believe that an unauthorized individual gained the ability to install malicious code designed to capture payment card information on certain pages of our website.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171208-01	CA Department of Rehabilitation	CA	12/1/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

On Wednesday, November 22, 2017, a file containing your name and social security number was inadvertently emailed without encryption to an outside entity. In performing our investigation, we determined that your name and social security number were contained within the emailed file.

Attribution 1 Publication: CA AG's office Author:
Article Title: CA Department of Rehabilitation
Article URL: https://oag.ca.gov/system/files/Notification%20Letter%20-%20%20Draft_12-4-17_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171207-03	W.W. Williams	OH	8/7/2017	Electronic	Business	Yes - Unknown #	Unknown

On July 6, 2017, one specific email account of an employee of W.W.Williams ("Williams") was targeted by an isolated scamming attempt. The scammer may have obtained access to a credit application which you submitted to Williams between the period of September 1, 2015 through July 7, 2017. That credit application contained your name and Social Security number. It may have also included your birth date, home address, home phone number, bank account information, and, potentially, your spouse's name.

Attribution 1 Publication: MD AG's office Author:
Article Title: W.W. Williams
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286557.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171207-02	**Sandpiper Property Management**	VA	8/10/2017	Electronic	Business	Yes - Unknown #	**Unknown**

The investigation thus far has produced evidence that someone had misappropriated the bank account and in some cases, social security numbers, of thirty-seven current and former Sandpiper employees.

Attribution 1 Publication: MD AG's office Author:
Article Title: Sandpiper Property Management
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286816%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171207-01	**State Street Group**	MA	8/8/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**Unknown**

On July 17, 2017, an employee of State Street inadvertently sent an encrypted email to two employees of an unrelated investment advisor. We have been informed by State Street that the information disclosed during this incident included the resident's name and taxpayer identification number, which may be their social security
number. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: State Street Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286560.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-13	**Ferrellgas**	KS	8/9/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Our investigation of the incident is ongoing, but it appears that an unauthorized person outside of Ferrellgas sent phishing emails to various Ferrellgas employees, enticing them to disclose their system access credentials. The information accessed includes personal information in your PeopleSoft online payroll account, such as your name, address, email address, birth date, Social Security number, bank information, benefits information, and healthcare summary information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Ferrellgas
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286565.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-12	**USAA Federal Savings Bank**	TX	8/8/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

pecifically, our representative accessed your USAA member information without authorization. Personal information involved in this incident included your your first and last name, address, phone number, email address, Social Security Number, date of birth, gender, marital status account password/user ID/security Q&A and account number ending in XXXX.

Attribution 1 Publication: MD AG's office Author:
Article Title: USAA Federal Savings Bank
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286814.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-11	**Skipper Law**	MD	8/15/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We are contacting you to inform you that Skipper Law was the subject of a ransomware computer virus attack on August 11, 2017. Our informational security technician has reviewed the system, and while our security was breached, we are fairly certain that no files or personal information were or will be accessed. Nonetheless, we wanted to notify you out of an abundance of caution to let you know of the incident.

Attribution 1 Publication: MD AG's office Author:
Article Title: Skipper Law
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286571%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-10	SafeRack	SC	8/17/2017	Electronic	Business	Yes - Unknown #	Unknown

On or about June 5, 2017, we learned that an unauthorized individual(s) may have gained access to an employee's email account. As part of our investigation, we conducted a thorough review of the contents of the employee's email account and identified some messages that contained some personal information, including name, address, date of birth, and Social Security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: SafeRack
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286598.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-09	Tax-On-Time, LLC	NJ	8/17/2017	Electronic	Business	Yes - Unknown #	Unknown

We discovered initially on June 6, 2017, that a data cyber-security incident involving our finn and some of our client's personal information occurred. Because the incident involved tax retum data, the personal information could include your name and social security number, as well as direct deposit banking information you may have provided to us, gender, date of birth, telephone number(s), address, employment (W-2) information, 1099 information, as well as correspondence and/or brokerage statements and other documents you provided to us to complete your tax return.

Attribution 1 Publication: MD AG's office / ME AG's officeus Author:
Article Title: Tax-On-Time, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286600.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-08	Davidson, Doyle & Hilton	VA	8/21/2017	Electronic	Business	Yes - Published #	1,474

On July 7, 2017, we became aware of suspicious activity on our computer systems. However, the investigation also determined that your name, address, Social Security number and tax information may have been viewed or accessed by an unknown third party.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Davidson, Doyle & Hilton
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286363.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-07	Taylor University	IN	8/23/2017	Electronic	Educational	Yes - Unknown #	Unknown

On July 26, 2017, we completed our investigation of a phishing email incident with the assistance of a leading computer forensics company. Our investigation determined that some of the information that you provided to Taylor University as part of your application for and/or participation in certain programs sponsored by the University was present in the compromised email accounts, which may have included your name, driver's license number or passport number, and, in some instances, medical history information.

Attribution 1 Publication: MD AG's office / ME AG's office Author:
Article Title: Taylor University
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286601.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-06	Jenu Biosciences	CA	8/18/2017	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that unauthorized individuals or entities installed malware that targeted our ecommerce platform on the Website. We believe the malware compromised the payment card data of certain customers who made payment card purchases through the Website during the time the malware was on the Website, including name, email address, billing/shipping address, phone number, payment card account number, card expiration date and security code

Attribution 1 Publication: MD AG's office Author:
Article Title: Jenu Biosciences
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286837.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-05	**Private Advisors Alternative Asset Management**	VA	8/10/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

During the brief window of unauthorized access, the unauthorized user may have had access to personal information, including name, address, and social security number of 1 Maryland resident.

Attribution 1 Publication: MD AG's office Author:
Article Title: Private Advisors
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286791.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-04	**American Para Medical Services**	NY	8/24/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

Although American Para Professional Systems, Inc. ("APPS") has implemented safeguards to protect the confidentiality of personal information, it was discovered that the personal information obtained with your examination for insurance on or about October, 2014 with New York Life may have been compromised. The information included your name, address, date of birth, and social security number.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: American Para Medical Services
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286789.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-03	**Gregory F. Wilt, CPA / Mario Bottoni, CPA / Advanced**	NY	8/31/2017	Electronic	Business	Yes - Published #	**1,856**

The forensic investigators found evidence of brief unauthorized access to one computer system. Based on our internal investigation of this matter, we have determined that the client information potentially at risk of being accessed includes first and last names, home addresses, social security numbers, tax return information, and financial account numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Gregory F. Wilt, CPA / Mario Bottoni, CPA / Advanced Financial Services, Inc. / Accu-Pay Payroll and Booking Services, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286849.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-02	**Henry Ford Health System**	MI	12/6/2017	Electronic	Medical/Healthcare	Yes - Published #	**18,470**

The Detroit-based Henry Ford Health System has started notifying almost 18,500 patients that some of their protected health information has potentially been accessed by an unauthorized individual. The emails contained a range of information on patients including names, medical record numbers, dates of birth, provider's name, department's name, location, dates of service, medical diagnoses, and the name of health insurers

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 18,500 Patients PHI Exposed After Multiple Email Accounts Were Compromised
Article URL: https://www.hipaajournal.com/18500-patients-phi-exposed-multiple-email-accounts-compromised/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171206-01	**JAM Paper & Envelope**	NJ	12/1/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On November 17, 2017, with the assistance of the cybersecurity firm, JAM determined that if a customer placed an order on its website from June 15, 2016 to November 6, 2017, information associated with the order being placed, including the customer's name, address, phone number, email address, payment card number, expiration date and security code (CVV) may have been obtained by an unauthorized third-party.

Attribution 1 Publication: OR AG's office Author:
Article Title: JAM Paper & Envelope
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1923526082

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171205-06	Baptist Health Louisville	KY	11/21/2017	Electronic	Medical/Healthcare	Yes - Published #	880

Baptist Health in Louisville, KY has notified 880 patients that some of their protected health information has potentially been accessed and stolen. A review of all emails in the account showed the types of information potentially compromised included names, medical record numbers, dates of birth, clinical information, and treatment information. A limited number of Social Security numbers were also exposed.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: 880 Patients Potentially Impacted by Baptist Health Louisville Phishing Attack
Article URL: https://www.hipaajournal.com/880-patients-baptist-health-louisville-phishing-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171205-05	Clinical Pathology Laboratories Southeast	FL	11/17/2017	Electronic	Medical/Healthcare	Yes - Published #	500

Clinical Pathology Laboratories Southeast FL Healthcare Provider 500 11/17/2017 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Clinical Pathology Laboratories Southeast
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=19D329571312B4EF61ECCF10516E47D6

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171205-04	Alere Toxicology	MA	11/28/2017	Paper Data	Medical/Healthcare	Yes - Published #	2,146

Alere Toxicology MA Healthcare Provider 2146 11/28/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Alere Toxicology
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=19D329571312B4EF61ECCF10516E47D6

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171205-03	UAB Medicine Viral Hepatitis Clinic	AL	12/1/2017	Electronic	Medical/Healthcare	Yes - Published #	652

UAB Medicine uses flash drives to transfer data from its Fibroscan machine to a computer. On October 25, 2017, two flash drives were discovered to be missing. Information stored on the devices included first and last names, gender, birth dates, images and numbers relating to test results, medical diagnosis, names of referring physician, and the dates and times of the examination.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: UAB Medicine Alerts 652 Patients of PHI Exposure
Article URL: https://www.hipaajournal.com/uab-medicine-652-patients-phi-exposure/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171205-02	Women's Health Consultants	PA	12/4/2017	Paper Data	Medical/Healthcare	Yes - Published #	Unknown

Paper files containing names, Social Security numbers, and medical histories, including details of cancer diagnoses and sexually transmitted diseases, have been dumped at a recycling center in Allentown, Pennsylvania.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Medical Records from Pennsylvania Obs/Gyn Clinic Found at Public Recycling Center
Article URL: https://www.hipaajournal.com/medical-records-pennsylvania-obsgyn-clinic-improper-disposal/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171205-01	County of Humboldt	CA	12/1/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

The Humboldt County Sheriff's Office recovered County of Humboldt payroll documents on September 7, 2017 while serving a search warrant in Trinity County. As a result of this review, we have confirmed that the recovered records included payroll records for some current and former employees of the county, as well as a limited group of dependents. As it pertains to you, the records include your full name and Social Security number.

Attribution 1 Publication: CA AG's office Author:
Article Title: County of Humboldt
Article URL: https://oag.ca.gov/system/files/Humboldt%20-%20FINAL%20PROOF%20-%20CA%20SSN%20%5Bredacted%5D%20%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171204-01	**Stanford University**	CA	12/1/2017	Electronic	Educational	Yes - Published #	**10,000**

On October 27, 2017, the University Privacy Office ("UPO") received a report that several folders with confidential information on a shared file server maintained by the Graduate School of Business ("GSB") were accessible to GSB faculty, staff and students. First name; last name; date of birth; Social Security Number; and, annual benefits base salary

Attribution 1 Publication: CA AG's office Author:
Article Title: Stanford University
Article URL: https://oag.ca.gov/system/files/Stanford%20Notification%20Letter_FINAL_11292017_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171129-06	**Ambrell Precision Induction Heating Solutions**	NY	4/6/2017	Electronic	Business	Yes - Unknown #	**Unknown**

In connection with this incident, an unauthorized third party unlawfull impersonated a company employee and obtained your personal information, along with the personal information of other Ambrell employees, via email communiation. The specific type of information contained within the w-2 forms include first and last name, address and the last four digits of each individuals' SSN.

Attribution 1 Publication: NY AG's office Author:
Article Title: Ambrell Precision Induction Heating Solutions
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171129-05	**Sallie Mae / SmartyPig LLC / Q2 Labs**	DE	11/9/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

On October 23, 2017, our third party service provider, SmartyPig LLC d/b/a 02 Labs, notifed us of attempts to access the residents' SmartyPig savings accounts from an unknown address through use of their login credentials fraudulently obtained from unknown sources. The information that may have been accessed includes: name, address, and Financial account number, in combination with the security code, access code, password, or PIN for the account.

Attribution 1 Publication: NH AG's office Author:
Article Title: Sallie Mae / SmartyPig LLC / Q2 Labs
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/smartypig-20171109.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171129-04	**Randolph Savings Bank**	MA	11/22/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

In October 2017, Randolph Savings discovered that an unauthorized individual gained access to certain emails belonging to Randolph Savings employees, the contents of which included information about some customers of Randolph Savings. Potentially-affected information includes names, addresses, loan numbers, and related information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Randolph Savings Bank
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/randolph-savings-20171121.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171129-03	**Boise Cascade Company**	ID	11/16/2017	Electronic	Business	Yes - Unknown #	**Unknown**

The Company's investigation determined that a phishing scheme got into its email system on or about October 31, 2017. The investigation further revealed that company-wide, 23 employees' direct deposit instructions were changed

Attribution 1 Publication: NH AG's office Author:
Article Title: Boise Cascade Company
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/boise-cascade-20171116.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171129-02	YMCA of Central Florida	FL	11/23/2017	Electronic	Business	Yes - Unknown #	Unknown

On October 24, 2017, the YMCA learned that an unauthorized person gained access to several employees' email accounts. At this time, the YMCA has no indication that the information in the emails was actually viewed or used in any way. However, out of an abundance of caution, the YMCA has notified potentially affected consumers. Individuals whose Social Security numbers were potentially involved will be offered a one-year, complimentary credit monitoring and identity protection service. In addition, the YMCA has established a dedicated call center to answer any questions individuals may have.

Attribution 1 Publication: databreaches.net / clickorlando.com Author:
Article Title: YMCA of Central Florida Notifies Individuals of Security Incident
Article URL: https://www.databreaches.net/ymca-of-central-florida-notifies-individuals-of-security-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171129-01	Humana Inc. / Real Time Health Quotes	KY	11/21/2017	Electronic	Medical/Healthcare	Yes - Published #	5,764

Humana Inc KY Health Plan 5764 11/21/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Humana Inc. / Real Time Health Quotes
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171128-01	Sports Medicine & Rehabilitation Therapy	MA	11/28/2017	Electronic	Medical/Healthcare	Yes - Published #	7,000

Massachusetts-based Sports Medicine & Rehabilitation Therapy (SMART) has alerted 7,000 patients to a breach of their protected health information

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 7,000 Patients Impacted by Extortion Attempt on Sports Medicine Provider
Article URL: https://www.hipaajournal.com/7000-patients-extortion-attempt-sports-medicine-provider/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171127-05	Uber / Users	CA	11/21/2017	Electronic	Business	Yes - Unknown #	Unknown

Uber disclosed Tuesday that hackers had stolen 57 million driver and rider accounts and that the company had kept the data breach secret for more than a year after paying a $100,000 ransom. The two hackers stole data about the company's riders and drivers — including phone numbers, email addresses and names — from a third-party server and then approached Uber and demanded $100,000 to delete their copy of the data, the employees said.

Attribution 1 Publication: nytimes.com / Uber website Author:
Article Title: Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data
Article URL: https://www.nytimes.com/2017/11/21/technology/uber-hack.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171127-04	NC Department of Health and Human Services	NC	11/24/2017	Electronic	Government/Military	Yes - Published #	6,000

A North Carolina agency says a spreadsheet containing personal information for nearly 6,000 people was sent in error to a vendor in an unencrypted email. The spreadsheet includes names, social security numbers and test results for people who underwent routine drug screenings for employment, intern and volunteer opportunities.

Attribution 1 Publication: witn.com / hipaajournal.com Author:
Article Title: NC Department of Health and Human Services
Article URL: http://www.witn.com/content/news/Thousands-could-be-victims-in-state-government-data-breech-459787643.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171127-03	ArmorGames	CA	10/24/2017	Electronic	Business	Yes - Unknown #	Unknown

On Oct 24, 2014, we discovered that a third party obtained access to our users' emails and "hashed' passwords. That means that the passwords were encrypted in such a way that it is nearly impossible for anyone, even us, to read it.

Attribution 1 Publication: CA AG's office Author:
Article Title: ArmorGames
Article URL: https://oag.ca.gov/system/files/DataBreachNotification_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171127-02	Uber / Drivers	CA	11/22/2017	Electronic	Business	Yes - Published #	600,000

In November 2016, Uber learned that unauthorized actors obtained access to a private cloud storage environment used by Uber. They accessed stored copies of Uber databases and files. The accessed files contained user information that Uber used to operate the Uber Information service, including your name and driver's license number. The files included this information for about 600,000 Uber drivers in the United States.

Attribution 1 Publication: CA AG's office / WI AG's office / MT AG' Author:
Article Title: Uber
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_0.PDF

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171127-01	Imgur	CA	11/27/2017	Electronic	Business	Yes - Unknown #	Unknown

On November 23, 2017, we were notified about a data breach that occurred in 2014. Based on our analysis, we believe that an unauthorized third party stole user account data from us. The stolen account information included your email address and password from 2014.

Attribution 1 Publication: CA AG's office Author:
Article Title: Imgur
Article URL: https://oag.ca.gov/system/files/Email%20for%20Impacted%20Users%20from%202014%20Data%20Breach_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171122-04	Indiana University Health (IU Health Ball Memorial Hospital)	IN	11/3/2017	Electronic	Medical/Healthcare	Yes - Published #	1,399

A bag of patient information was lost for several days and recovered along McGalliard Road in Muncie, IU Health Ball Memorial Hospital has announced. "The paperwork may have contained patient names, dates of birth, physicians names, medical record numbers, diagnoses, procedures, gender and dates and times of service," the hospital said.

Attribution 1 Publication: hhs.gov Author:
Article Title: Indiana University Health (IU Health Ball Memorial 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
ITRC20171122-03	Center for Health Care Services	TX	11/8/2017	Paper Data	Medical/Healthcare	Yes - Published #	28,434

Center for Health Care Services (CHCS) in San Antonio, a provider of mental health treatment and support services for individuals with intellectual and developmental disabilities, has discovered documents containing the protected health information of patients have been stolen by a former employee. The data included names, dates of birth, addresses, Social Security numbers, dates and types of services, medical record numbers, referral information, progress notes, medical diagnoses, medications prescribed, treatment plans, laboratory and toxicology reports, death certificates, autopsy reports, discharge dates, death summaries, and collateral hospital information.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: PHI of 28,000 Mental Health Patients Stolen by Healthcare Employee
Article URL: https://www.hipaajournal.com/phi-28000-mental-health-patients-stolen-by-healthcare-employee/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171122-02	**Family & Cosmetic Dentistry of the Rockies**	CO	11/13/2017	Paper Data	Medical/Healthcare	Yes - Published #	**1,850**

Family & Cosmetic Dentistry of the Rockies CO Healthcare Provider 1850 11/13/2017 Improper Disposal Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Family & Cosmetic Dentistry of the Rockies
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171122-01	**Lowell General Hospital**	MA	11/10/2017	Electronic	Medical/Healthcare	Yes - Published #	**769**

Lowell General Hospital in Massachusetts has discovered the medical records of 769 patients have been accessed by an employee without any legitimate work reason for doing so. Patients have been informed that the types of information accessed by the former employee included names, dates of birth, medical diagnoses, and information relating to treatments provided to patients.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Lowell General 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
ITRC20171121-06	**Missions Door**	CO	11/3/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Since completing our investigation and manual document review, which concluded on or about October 5, 2017, we concluded that an unauthorized third party accessed the email account at issue. Because we value our relationship with you, we wanted to notify you of this incident since your personal information was contained within the compromised email account, which included your full name and Social Security number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Missions Door
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/missions-door-20171103.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171121-05	**Oppenheimer Funds**	CO	11/14/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

It is important for us to share with you that on November 3, 2017, Oppenheimer Funds was made aware of an incident which occurred between May 24, 2011 and October 16, 2017, in which certain information relating to you and your OppenheimerFunds account (including your name, address, Social Security number, and account number) was erroneously sent to a financial services firm with which OppenheimerFunds maintains an ongoing business relationship.

Attribution 1 Publication: NH AG's office Author:
Article Title: Oppenheimer Funds
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/oppenheimer-20171114.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171121-04	**Department of Social and Health Services' Behavioral**	WA	11/16/2017	Electronic	Government/Military	Yes - Published #	**515**

On September 20, 2017, the breach was discovered after an employee at Western State Hospital discovered they had sent a document containing client health history to an incorrect email address. Personal health information such as names of patients, admission dates to Western State Hospital, the Western State Hospital medical record number, date of birth as well as specific diagnosis of infection were included on the spreadshee

Attribution 1 Publication: q13fox.com Author:
Article Title: Western State Hospital patient information sent to wrong email address
Article URL: http://q13fox.com/2017/11/16/western-state-hospital-patient-information-sent-to-wrong-email-address/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171121-03	**Rocky Mountain Health Care Services (9/17)**	CO	11/21/2017	Electronic	Medical/Healthcare	Yes - Published #	**909**

Rocky Mountain Health Care Services of Colorado Springs has discovered an unencrypted laptop has been stolen from one of its employees. This is the second such incident to be discovered in the space of three months. The types of information stored on the device included first and last names, addresses, dates of birth, health insurance information, Medicare numbers, and limited treatment information.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Second Unencrypted Laptop Stolen from Rocky Mountain Health Care Services
Article URL: Second Unencrypted Laptop Stolen from Rocky Mountain Health Care Services

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171121-02	**Medical College of Wisconsin**	WI	11/18/2017	Electronic	Medical/Healthcare	Yes - Published #	**9,500**

An unauthorized third party accessed employee email accounts, which contained private patient information such as their date of birth, home address, medical record numbers and diagnosis. The information includes addresses, bank accounts and Social Security numbers.

Attribution 1 Publication: hipaajournal.com / OR AG's office Author:
Article Title: 9,500 Patients Impacted by Medical College of Wisconsin Phishing Attack
Article URL: https://www.hipaajournal.com/9500-medical-college-of-wisconsin-phishing-attack/

Attribution 2 Publication: WQOW. Com / hipaajournal.com Author:
Article Title: Medical College of Wisconsin hit by data security breach
Article URL: http://www.wqow.com/story/36879172/2017/11/Saturday/medical-college-of-wisconsin-hit-by-data-security-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171121-01	**USA Hoist Company, Inc. / Mid-American Elevator**	IL	11/14/2017	Electronic	Business	Yes - Unknown #	**Unknown**

A server used by USA Hoist Company, Inc., Mid-American Elevator
Company, Inc., and Mid-American Elevator Equipment Company, Inc. to store employee and vendor information was subject to a ransomware attack by the hacker group called "the Dark Overlord." (TDO) The information breached contained employee names, mailing addresses, cancelled checks for employee direct deposits, direct payment account
numbers for employees and vendors, non-union member employee health insurance applications, and/or employee Social Security numbers.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: USA Hoist Company, Inc. / Mid-American Elevator Company, Inc. / Mid-American Elevator Equipment Company, Inc.
Article URL: https://oag.ca.gov/system/files/USA%20Hoist%20-%20Data%20Security%20Breach%20Notification%20Form_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171120-09	**Otolaryngology Associates of Central Jersey**	NJ	11/17/2017	Paper Data	Medical/Healthcare	Yes - Published #	**1,551**

Otolaryngology Associates of Central Jersey is alerting patients to a breach of their protected health information, following a burglary at an off-site storage facility in East Brunswick, NJ. The thieves took 13 boxes of paper medical records from the facility, which included information such as names, addresses, health insurance account numbers, birth dates, dates of military service, and the names of treating physicians. A limited number of driver's license numbers and Social Security numbers were also included in the stolen records.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Boxes of Medical Records Stolen from New Jersey Medical Practice
Article URL: https://www.hipaajournal.com/medical-records-stolen-new-jersey-medical-practice/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171120-08	**UPMC Susquehanna**	PA	11/20/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,200**

While details of the breach date have not been released, UPMC Susquehanna says it discovered the breach on September 21, when an employee reported suspicious activity on their computer. It is not known whether the attacker viewed, stole, or misused any patient information, but the possibility of data access and misuse could not be ruled out. The information potentially accessed includes names, contact information, dates of birth, and Social Security numbers.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Suspected Phishing Attack on UPMC Susquehanna Exposes 1,200 Patients' PHI
Article URL: https://www.hipaajournal.com/phishing-attack-upmc-susquehanna/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171120-07	Saris Cycling Group	WI	11/15/2017	Electronic	Business	Yes - Unknown #	Unknown

On or about October 18, 2017, we discovered that Saris had become the target of a phishing email campaign and that an employee had clicked on phishing emails and entered their credentials. While we currently have no evidence that the unauthorized individual or individuals actually accessed or acquired your information, we have confirmed that your name, address and Social Security number were accessible to the unknown actor during this event.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171120-06	GCI / The Siegfried Group	AK	11/13/2017	Electronic	Business	Yes - Unknown #	Unknown

Last Thursday, November 2, 2017 The Siegfried Group, an outside contract services firm that provides accounting contractors to GCI, notified us that one of its accountants had downloaded a limited amount
of GCI data from a restricted folder onto an external drive without permission or authorization to do so. The stolen information included a 2015 GCI report used to track accrued employee vacation amounts
and listed employee names and Social Security numbers.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171120-05	Brinderson, an Aegion Company	CA	10/24/2017	Electronic	Business	Yes - Unknown #	Unknown

On October 24, 2017, we discovered that an unauthorized individual may have gained access to one of our computer systems. Our investigation has determined that some of your information was stored on systems potentially accessed by the unauthorized individual. That information includes your name, address, Social Security number, date of birth, and other employment related information.

Attribution 1 Publication: CA AG's office / NH AG's office / MT AG' Author:
Article Title: Brinderson, an Aegion Company
Article URL: https://oag.ca.gov/system/files/T425_v01%20-%20CA%20Notice_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171120-04	Academy of Art University	CA	11/17/2017	Electronic	Educational	Yes - Unknown #	Unknown

On November 8, 2017, an Academy employee mistakenly sent an internal e-mail with an attachment (subject of email: Reminder! 2017 Difference Card Reimbursement Claims), and one of the spreadsheet tabs included in the attachment contained your personal information. The attachment to the e-mail contained several spreadsheet tabs, one of which listed your first name, last name, and Social Security number.

Attribution 1 Publication: CA AG's office Author:
Article Title: Academy of Art University
Article URL: https://oag.ca.gov/system/files/TEMPLATE%20Notice%20to%20Employees%20%28All%20except%20Mass%20Oregon

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171120-03	ClubSport San Ramon / Oakwood Athletic Club	CA	8/9/2017	Electronic	Business	Yes - Unknown #	Unknown

On July 31, 2017, we discovered that an employee was the subject of a phishing attack when they received an email that appeared to be from an executive, requesting copies of employees W-2 wage and tax statements. In response to that email, individual employee W-2 information was sent to an unauthorized email address.

Attribution 1 Publication: CA AG's office Author:
Article Title: ClubSport San Ramon / Oakwood Athletic Club
Article URL: https://oag.ca.gov/system/files/SFDOCS01-%231811613-v1-ClubSport---Notice-to-Employees-Final_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171120-02	Far Niente Winery	CA	8/21/2017	Electronic	Business	Yes - Unknown #	Unknown

On August 21, 2017, files on Far Niente's computers were encrypted by an individual who gained unauthorized access to Far Niente's computer network. However, your name, address, and Social Security number were included in a document on the network.

Attribution 1 Publication: CA AG's office Author:
Article Title: Far Niente Winery
Article URL: https://oag.ca.gov/system/files/Far%20Niente%20CA%20notification_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171120-01	CMI Marketing, Inc. dba Café Media / CaféMom	NY	11/15/2017	Electronic	Business	Yes - Unknown #	Unknown

Our investigation showed that email addresses and passwords for CafeMom accounts created before July 2011 were compromised at some point in the past.

Attribution 1 Publication: CA AG's office Author:
Article Title: CMI Marketing, Inc. dba Café Media / CaféMom
Article URL: https://oag.ca.gov/system/files/CafeMom%20Email%2011-6-17_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171115-02	North American Title Company	FL	11/3/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Through our investigation, we determined that an unauthorized party obtained access to an email account belonging to a North American Title
Company employee between June 27, 2017 and August 16, 2017. As a result, the unauthorized party may have been able to view some of your information maintained by us in connection with your real estate transaction that we closed, including your name and Social Security number.

Attribution 1 Publication: NH AG's office Author:
Article Title: North American Title Company
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/north-american-title-20171103.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171115-01	Forever 21	CA	11/11/2017	Electronic	Business	Yes - Unknown #	Unknown

Forever 21 is notifying its customers that it recently received a report from a third party that suggested there may have been unauthorized access to data from payment cards that were used at certain Forever 21 stores. The company's investigation is focused on card transactions in Forever 21 stores from March 2017 – October 2017. Because the investigation is continuing, complete findings are not available, and it is too early to provide further details on the investigation.

Attribution 1 Publication: Forever 21 press release / NH AG's offic Author:
Article Title: Notice of Payment Card Security Incident
Article URL: https://www.prnewswire.com/news-releases/notice-of-payment-card-security-incident-300555878.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-13	Utah Department of Transportation Express Pass	UT	11/10/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

A vigilant UDOT Express Pass customer discovered a glaring security breach in the third-party website that manages pass accounts, but state officials don't yet know if the personal information of approximately 21,000 current and former customers has been compromised. That information on customers who have purchased passes for accessing HOV lanes includes names and addresses, phone numbers, and credit card information — including the last four digits of account numbers and expiration dates, and even the security question and answer associated with the account.

Attribution 1 Publication: databreaches.net / desertnews.vom Author:
Article Title: Security flaw may have exposed personal info on 21,000 Utah Express Pass users
Article URL: https://www.deseretnews.com/article/900003671/security-flaw-may-have-exposed-personal-info-on-21000-utah-express

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-12	Fasten	ME	11/10/2017	Electronic	Business	Yes - Unknown #	Unknown

The company has confirmed that it was notified late last month of a potential data breach. Among the data viewed by a security researcher were the names, email addresses and phone numbers of customers, as well as links to their photos. The last four digits of the customers' credit cards or email addresses associated with their PayPal accounts were also included. Moreover, the car registration information and license plate details of Fasten's drivers were discovered in the cache, sitting online, without the protection of a password.

Attribution 1 Publication: gizmodo.com Author:
Article Title: Ride-Hailing Service Prominent at SXSW Briefly Exposed Data on as Many as 1 Million Customers
Article URL: https://gizmodo.com/ride-hailing-service-prominent-at-sxsw-briefly-exposed-1820335380

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-11	Maine Office of Information Technology / Knowledge	ME	11/13/2017	Electronic	Government/Military	Yes - Published #	2,100

The office "has begun notifying approximately 2,100 individuals of a recent incident that may have resulted in a temporary exposure of their personal information," the agency said in a statement.

Attribution 1 Publication: databreaches.net / sunjournal.com Author:
Article Title: Social Security numbers of 2,100 Maine foster care participants posted online
Article URL: http://www.sunjournal.com/social-security-numbers-of-2100-maine-foster-care-participants-posted-online/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-10	Florida Blue / Real Time Health Quotes	FL	10/27/2017	Paper Data	Medical/Healthcare	Yes - Published #	939

Blue Cross and Blue Shield of Florida, dba Florida Blue, has announced that the personally identifiable information of a limited number of insurance applicants has been exposed online. The files contained information such as the names of applicants, dates of birth, demographic information, medical histories, Social Security numbers, and limited banking and payment information.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Florida Blue Data Breach Impacts 939 Individuals
Article URL: https://www.hipaajournal.com/florida-blue-data-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-09	Bakersfield City School District	CA	11/13/2017	Electronic	Educational	Yes - Published #	1,250

On November 9, 2017, at or about 4:24 p.m., the Board Docs Agenda was posted to the District's website. The personal information potentially compromised includes their names and Social Security numbers.

Attribution 1 Publication: CA AG's office Author:
Article Title: Bakersfield City School District
Article URL: https://oag.ca.gov/system/files/Employee%20Letter%20regarding%20Data%20Breach_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-08	ABM Industries Incorporated	NY	11/14/2017	Electronic	Business	Yes - Unknown #	Unknown

On or about August 1, 2017, we discovered that ABM had become the target of a phishing email campaign. What Information Was Involved? While we currently have no evidence that the unauthorized individual or individuals actually accessed or acquired your information, we have confirmed that your name<<ClientDef1(data elements affected)>> accessible within the affected email accounts.

Attribution 1 Publication: CA AG's office / MT AG's office / VT AG' Author:
Article Title: ABM Industries Incorporated
Article URL: https://oag.ca.gov/system/files/ABM%20-%20Notice%20only%200_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-07	**East Central Kansas Area Agency on Aging**	KS	10/31/2017	Electronic	Business	Yes - Published #	**8,750**

East Central Kansas Area Agency on Aging was the victim of a computer breach earlier this fall. The breach at ECKAAA, 117 S. Main, Ottawa, occurred Sept. 5. Files containing names, address, telephone number, birthdate, social security number and/or Medicaid number were encrypted by ransomware, which means the agency could not “open or access the encrypted files,” a news release said.

Attribution 1 Publication: hhs.gov / ottawaherald.com Author:
Article Title: Agency’s data remains uncompromised after computer breach
Article URL: http://www.ottawaherald.com/news/20171102/agencys-data-remains-uncompromised-after-computer-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-05	**Wilbraham, Lawler and Buba, P.C.**	PA	11/3/2017	Electronic	Business	Yes - Unknown #	**Unknown**

In the course of such an action, we received personal information regarding you. WLB was recently the subject of a "ransomware" attack, which resulted in the encryption of all of the data on our servers. Depending on the specifics of a given situation, the types of personal information in our systems may have included names and some combination of the following: Social Security numbers, addresses, medical information, employment information, driver's license information, settlement documentation and dates of birth.

Attribution 1 Publication: VT AG's office / NH AG's office Author:
Article Title: Wilbraham, Lawler and Buba, P.C.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Wilbraham%20Lawler%20&%20Buba%20PC%20SBN%

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-04	**InTouch Credit Union**	TX	11/8/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

Earlier this year, InTouch Credit Union worked with a third-party vendor to provide data analytics services.On October 10, 2017, this vendor notified us that it was the victim of a ransomware attack and files containing InTouch Credit Union member information may have been affected. The following information about you was affected and may have been subject to unauthorized access or acquisition: Social Security number, financial account information, loan account information, and name.

Attribution 1 Publication: MT AG's office / VT AG's office Author:
Article Title: InTouch Credit Union
Article URL: https://dojmt.gov/wp-content/uploads/InTouch-Credit-Union.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-03	**Los Angeles County Department of Mental Health**	CA	11/13/2017	Electronic	Government/Military	Yes - Unknown #	**Unknown**

On October 24, 2017, a LACDMH employee sent an email to candidates who responded to a job posting for a position within LACDMH. Inadvertently attached to that email was a spreadsheet that contained the PII of candidates, including you. The information that may have been compromised included your name, promulgation date, email address, and Social Security Number.

Attribution 1 Publication: CA AG's office Author:
Article Title: Los Angeles County Department of Mental Health
Article URL: https://oag.ca.gov/system/files/NOTICE%20OF%20DATA%20BREACH%20LETTER%20-%20LACDMH_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-02	**Gallagher NAC (multiple data owners)**	IL	9/19/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On September 21, 2017, our system monitoring tools identified unusual activity relating to a database within our network that is tied to a web application used by GNAC customers, including [DATA OWNER].
While our investigation is ongoing, we wanted to inform you that information of yours contained in the database during the period in question included your name and Social Security number.

Attribution 1 Publication: CA AG's office / VT AG's office / MT AG' Author:
Article Title: Gallagher NAC
Article URL: https://oag.ca.gov/system/files/GNAC%20-%20Notice%20only%20-%20Exhibit%201%20-%20CA_0_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171114-01	**Dignity Health / Mercy San Juan Medical Center**	CA	11/13/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

We want to make you aware that from September 8-12th· 2017 some of your employee personal information was inadvertently exposed and may have been seen by other Dignity Health employees who accessed the Employee Self Service (ESS) system.

Attribution 1 Publication: CA AG's office Author:
Article Title: Dignity Health / Mercy San Juan Medical Center
Article URL: https://oag.ca.gov/system/files/Dignity%20Health%20sample%20notice%20ESS%20Incident%20Individual%20Notif%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171113-05	**Rain Bird Corporation**	CA	11/3/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We were recently alerted that certain Rain Bird customers were experiencing technical issues when completing an online purchase on the Rain Bird store website. We promptly began investigating this incident and engaged a third party computer forensic firm to assist with determining what may have happened. Based upon the forensic firm's investigation, it appears that an unauthorized individual was able to gain access to portions of our store website between August 25, 2017 and September 15, 2017 and install malicious software on certain pages that was designed to capture payment card information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171113-04	**GlaxoSmithKline Patient Assistance Program**	NJ	10/31/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

The company that manages the Program administration, The Lash Group, Inc. ("Lash Group"), learned on September 5 that one if its former employees may have accessed your personal information and that it may have been used for fraudulent purposes. The information that may have been disclosed may have included your social security number, name, address, credit history, employment information, and date of birth.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171113-03	**Gary W. Janke**	CA	10/17/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On the night of September 26, 2017, a thief broke into the back of the office building in Northridge, California. Unfortunately, he stole two old computers from my offices. The computers contained tax information from 2012 and prior year tax returns that I had prepared. The data on the computers contained your personal information, including your name(s), address, Social Security number(s) and date of birth. It also included dependent information including name, social security number and date of birth. (For business clients, the data would have included federal identification numbers.)

Attribution 1 Publication: CA AG's office Author:
Article Title: Gary W. Janke
Article URL: https://oag.ca.gov/system/files/Data%20Breach%20notification%20%2010-17-17_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171113-02	**Corovan/Corodata/Klinger/Employer Leasing**	CA	11/7/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On October 17, 2017, we became aware that certain Company files containing sensitive information that were stored on a Company server had become browsable for a brief period of time through a directed search on the Google search engine. As part of the investigation into this incident, we determined a file containing the following information related to you was temporarily accessible through a directed search on Google: name, address, <<Data Elements Impacted>>.

Attribution 1 Publication: CA AG's office Author:
Article Title: Corovan/Corodata/Klinger/Employer Leasing
Article URL: https://oag.ca.gov/system/files/Corovan%20-%20notice%20onlyL_0_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171113-01	**Chapman University's Harry and Diane Rinker Health**	CA	10/28/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

Last week an external hard drive went missing from Chapman University's Harry and Diane Rinker Health Science Campus. I regret to inform you that a copy of your W9 form was among the content found on the network drives that could have been accessed and downloaded to the external drive.

Attribution 1 Publication: CA AG's office Author:
Article Title: Chapman University's Harry and Diane Rinker Health Science Campus
Article URL: https://oag.ca.gov/system/files/Form%20of%20Notice%20Letter%20Regarding%20Breach_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171107-04	**Kaiser Foundation Health Plan (10/2017)**	CA	10/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	**720**

Kaiser Foundation Health Plan CA Health Plan 720 10/20/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Kaiser Foundation Health Plan (10/2017)
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171107-03	**Emergency Coverage Corporation**	TN	10/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	**719**

EMERGENCY COVERAGE CORPORATION TN Healthcare Provider 719 10/20/2017 Loss Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Emergency Coverage 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
ITRC20171107-02	**Aetna (10/23/2017)**	CT	10/23/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,506**

Aetna, Inc. CT Health Plan 1506 10/23/2017 Unauthorized Access/Disclosure Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Aetna (10/23/2017)
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171107-01	**Arch City Dental, LLC - Drs. Baloy and Donatelli**	OH	10/26/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,716**

Arch City Dental, LLC - Drs. Baloy and Donatelli OH Healthcare Provider 1716 10/26/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Arch City Dental, LLC - Drs. Baloy and Donatelli
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171106-07	**Southern National Bancorp of Virginia, Inc. dba Sonabank**	VA	10/31/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

On or about July 27, 2017, Sonabank discovered suspicious activity related to its email system. Upon further investigation, Sonabank determined that beginning on or about June 8, 2017 and continuing through July, certain Sonabank employees received multiple phishing emails designed to harvest credentials.

Attribution 1 Publication: NH AG's office / VT AG's office / MT AG' Author:
Article Title: Southern National Bancorp of Virginia, Inc. dba Sonabank
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/southern-national-bancorp-20171031.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171106-06	LPL Financial (9/17)	CA	10/3/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On September 20, 2017, LPL Financial (LPL) received notice from one of its third-party audit firms that the audit firm experienced an email compromise. The service provider reported that the email accounts involved may have contained the personal information of certain LPL clients. Findings from the investigation show that the email accounts contained the personal information of one New Hampshire resident, including name, address, Social Security number and LPL account number.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: LPL Financial (9/20/17)
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/lpl-financial-20171003.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171106-05	NH Department of Health and Human Services	NH	10/30/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

On September 8, 2017 we became aware that the personal information of three (3) New Hampshire residents was accessed by an unauthorized State employee at the Department of Health and Human Services (D HHS), Berlin District Office. The information accessed included the residents' names, addresses, telephone numbers, dates of birth and social security numbers.

Attribution 1 Publication: NH AG's office Author:
Article Title: NH Department of Health and Human Services
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/deparatment-health-human-services-20171030.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171106-04	Valley Family Medicine	VA	11/3/2017	Electronic	Medical/Healthcare	Yes - Published #	8,450

Two employees printed and misused a mailing list of 8,450 patient names and addresses. The only information the printed mailing list contained were names and addresses — no other identifying data, health or financial information were included, the press release said.

Attribution 1 Publication: newsleader.com / hipaajournal.com Author:
Article Title: Staunton medical practice reports patient data breach
Article URL: http://www.newsleader.com/story/news/local/2017/11/03/valley-family-medicine-reports-patient-data-breach/830753001

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171106-02	TJ Samson Community Hospital	KY	11/4/2017	Electronic	Medical/Healthcare	Yes - Published #	683

An independent care provider who provides care to patients of TJ Samson Community Hospital in South Central Kentucky, has been discovered to have inappropriately accessed the protected health information (PHI) of 683 patients of TJ Samson Community Hospital in Glasgow, KY and the TJ Health Columbia Clinic. The types of information accessed included names, medical information, demographic information, and in some cases, Social Security numbers and insurance information.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: TJ Samson Community Hospital Discovers Inappropriate Accessing of 683 Patients' PHI
Article URL: https://www.hipaajournal.com/tj-samson-community-hospital-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171106-01	Tween Brands (formerly Too, Inc.)	OH	11/6/2017	Electronic	Business	Yes - Unknown #	Unknown

On September 7, 2017, we discovered signs indicating attempts had been made to gain access to one of our web servers. The database included information regarding current and former Tween Brands associates, including your name, date of birth, and Social Security number.

Attribution 1 Publication: CA AG's office / OR AG's office / MT AG Author:
Article Title: Tween Brands
Article URL: https://oag.ca.gov/system/files/Tween%20Brands%20Notification%20CA1%20and%20CA2_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171103-01	Kimberly-Clark	WI	10/30/2017	Electronic	Business	Yes - Unknown #	Unknown

We have extensive measures in place to protect the information that you provide to us; however, around October 20th, 2017 we identified an organized effort to access registered accounts on our website/app around October 18 using a list of 10 and password combinations that appears to have been obtained from other compromised sites not related to Kimberly-Clark nor any of its brands like Huggies or Kleenex, etc.

Attribution 1
Publication: CA AG's office Author:
Article Title: Kimberly-Clark
Article URL: https://oag.ca.gov/system/files/Kimberly-Clark%20Cyber%20Event%20Letter%20-%20Oct%202017%20-%20US_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171101-08	Menchinger & Tyack, CPAs, LLC	FL	11/1/2017	Electronic	Business	Yes - Unknown #	Unknown

Menchinger & Tyack recently learned that an unauthorized individual may have accessed information related to some of Menchinger & Tyack's clients. The investigation concluded on April 25, 2017, and Menchinger & Tyack determined that some of Menchinger & Tyack's clients' and their family members' names, addresses, and Social Security numbers were included on tax return information that may have been subject to potential unauthorized access.

Attribution 1
Publication: CT AG's Office Author:
Article Title: Menchinger & Tyack, CPAs, LLC
Article URL: Per CT FOIA request

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171101-07	Creighton University Trio program	NE	10/25/2017	Paper Data	Educational	Yes - Unknown #	Unknown

A number of Omaha parents are now upset about a recent data breach at Creighton University. "A lot of the kids information on it, all the way from first name, last name, social security numbers, grades, email address, phone numbers and date of birth."

Attribution 1
Publication: databreaches.net / crossroadstoday.com Author:
Article Title: Student information leaked from Creighton University Trio program
Article URL: http://www.crossroadstoday.com/story/36683166/student-information-leaked-from-creighton-university-trio-program

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171101-06	Midland County	TX	10/27/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

The Midland County District Attorney is warning residents after their third-party payment system was hacked. Since the forensic investigation was not conducted by the vendor, Midland County isn't aware of the extent, if any, of the information exposed. They are, however, not ruling out that possibility at this time.

Attribution 1
Publication: databreaches.net/ newswest9.com Author:
Article Title: Personal information possibly compromised for people paying fines, fees to Midland County
Article URL: http://www.newswest9.com/story/36701314/personal-information-possibly-compromised-for-people-paying-fines-fees-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171101-05	Catholic Charities of the Diocese of Albany - Glen Falls	NY	10/27/2017	Electronic	Business	Yes - Published #	4,624

The personal information of about 4,600 past and present clients and several employees of Catholic Charities may have been exposed after a computer server in the Glens Falls office was hacked, according to Catholic Charities for the Diocese of Albany. A technology firm called in to investigate the matter determined that information, including birth dates, dates of service and diagnosis codes and Social Security numbers, stored on the server may have been accessed.

Attribution 1
Publication: databreaches.net / timesunion.com Author:
Article Title: Computer server in Catholic Charities' Glens Falls office targeted by hackers
Article URL: http://www.timesunion.com/news/article/Catholic-Charities-warns-clients-and-employees-of-12312578.php

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171101-04	Memory4Less	CA	10/24/2017	Electronic	Business	Yes - Unknown #	Unknown

Our investigation revealed that between November 2016 and September 2017, an intruder installed malicious software onto our network, which led to the compromise of some of our customers' personal information. The personal information involved includes your name, e-mail address, credit card number that was used to purchase Memory4Less products, billing address, shipping address, and your FedEx/UPS account number (if a shipping account number was provided).

Attribution 1
Publication: MT AG's office / NH AG's office Author:
Article Title: Memory4Less
Article URL: https://dojmt.gov/wp-content/uploads/Memory4Less.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171101-03	Recovery Institute of the South East, P.A.	FL	10/21/2017	Electronic	Medical/Healthcare	Yes - Published #	689

Recovery Institute of the South East P.A. FL Healthcare Provider 689 10/21/2017 Hacking/IT Incident Desktop Computer, Electronic Medical Record, Email, Laptop, Network Server, Other, Other Portable Electronic Device, Paper/Films

Attribution 1
Publication: hhs.gov Author:
Article Title: Recovery Institute of the South East, 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
ITRC20171101-02	Interstate Plastics	CA	10/27/2017	Electronic	Business	Yes - Unknown #	Unknown

On or around July 24, 2017, we identified suspicious code on our e-commerce site and determined it was a sign of a sophisticated cyber-attack. The investigation has determined the following information could be collected by the malicious code: name, address, card number, expiration date, and CVV.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171101-01	Human Good	CA	10/17/2017	Electronic	Business	Yes - Unknown #	Unknown

On September 27, 2017, HumanGood learned that an unauthorized individual may have accessed personal information of certain HumanGood employees maintained by a third-party benefits coordination vendor.

Attribution 1
Publication: MT AG's office / CA AG's office / NH AG' Author:
Article Title: Human Good
Article URL: https://dojmt.gov/wp-content/uploads/Human-Good.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171031-07	Texas Children's Health Plan	TX	10/27/2017	Electronic	Medical/Healthcare	Yes - Published #	932

The protected health information (PHI) of 932 members of the Texas Children's Health Plan has been discovered to have been emailed to the personal email account of a former employee. The types of data included in the emails varied for each patient, but typically included: Names, telephone numbers, addresses, dates of birth, Medicaid numbers, waiver type, STAR kids manager's name and group, and information detailed in a budget worksheet.

Attribution 1
Publication: hhs.gov / hipaajournal.com Author:
Article Title: 932 Texas Children's Health Plan Members' PHI Emailed to Personal Account by Employee
Article URL: https://www.hipaajournal.com/texas-childrens-health-plan-phi-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171031-06	MGA Home Healthcare Colorado, Inc.	AZ	10/25/2017	Electronic	Medical/Healthcare	Yes - Published #	2,898

MGA Home Healthcare Colorado, Inc. AZ Healthcare Provider 2898 10/25/2017 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
Article Title: MGA Home Healthcare Colorado, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=DDD85E9B7ECB0D8D50C5A539BB14C388

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171031-05	Martinsville Henry County Coalition for Health and	VA	10/13/2017	Electronic	Medical/Healthcare	Yes - Published #	5,806

MHC Coalition for Health and Wellness VA Healthcare Provider 5806 10/13/2017 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: MHC Coalition for Health and Wellness
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=DDD85E9B7ECB0D8D50C5A539BB14C388

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171031-04	Insulet Corporation	MA	10/17/2017	Electronic	Medical/Healthcare	Yes - Published #	1,469

Insulet Corporation MA Healthcare Provider 1469 10/17/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Insulet Corporation
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=DDD85E9B7ECB0D8D50C5A539BB14C388

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171031-03	Aetna, Inc.	CT	10/23/2017	Electronic	Medical/Healthcare	Yes - Published #	1,506

Aetna, Inc. CT Health Plan 1506 10/23/2017 Unauthorized Access/Disclosure Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Aetna, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=DDD85E9B7ECB0D8D50C5A539BB14C388

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171031-02	Brevard Physician Associates	FL	10/24/2017	Electronic	Medical/Healthcare	Yes - Published #	7,976

A limited amount of protected health information (PHI) of almost 8,000 patients of Brevard Physician Associates has been exposed after a desktop computer was stolen in a burglary. In total, 7,976 patients were potentially impacted and had the following information exposed: Names, names of insurance providers, CPT codes for the services provided, and the amounts charged for services.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: 8,000 Patients Notified of PHI Exposure After Office Burglary
Article URL: https://www.hipaajournal.com/8000-patients-phi-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171031-01	Home Box Office (HBO)	NY	10/31/2017	Electronic	Business	Yes - Unknown #	Unknown

In late July 2017, HBO became aware of an incident in which an unauthorized third party claimed to have accessed HBO's information technology network. Though the investigation is still underway, we have determined that the information involved in this incident included the following types of your personally identifiable information: [Personal Information Categories]. According to WI breach notification, information include SSN's.

Attribution 1 Publication: CA AG's office / NH AG's office / WI AG' Author:
Article Title: Home Box Office
Article URL: https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171030-05	Advisory Research Investment Management	IL	10/24/2017	Electronic	Business	Yes - Published #	Unknown

On October 11, 2017, Advisory Research became aware that certain account information for a limited number of clients was accessible in the structural architecture of our website. The accessible account information included client name, custodian, and custodian account number.

Attribution 1 Publication: MT AG's office / NH AG's office / ME AG Author:
Article Title: Advisory Research Investment Management
Article URL: https://dojmt.gov/wp-content/uploads/Advisory-Research.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171030-04	BMT Designers & Planners	VA	10/16/2017	Electronic	Business	Yes - Published #	Unknown

While the FBI informed us that this attack was most likely intended to target our proprietary data, we were also notified that the hacker accessed a server used by our timekeeping system containing personal information of current and former employees. Specifically, the breached timekeeping server contained your name, social security number, date of hire, employee number and wage information. It did not, however contain your date of birth, address, yearly W2 or any direct deposit of bank account information.

Attribution 1 Publication: MT AG's office / ME AG's office Author:
Article Title: https://dojmt.gov/wp-content/uploads/Designers-and-Planners.pdf
Article URL: https://dojmt.gov/wp-content/uploads/Designers-and-Planners.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171030-03	Mark Schaefer Associates, LLP	CA	10/16/2017	Electronic	Business	Yes - Unknown #	Unknown

On September 9, 2017, MSA discovered it was the target of a break-in which resulted in the theft of two external hard drives among other low value items which do not have the capability to store information or data. The personal information subject to this incident may include name, address, Social Security number, and financial information from prior to 2013.

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: Mark Schaefer Associates, LLP
Article URL: https://dojmt.gov/wp-content/uploads/Mark-Schaefer-Associates-1.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171030-02	Union Labor Life Insurance Company	CA	9/28/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 22, 2017, The Union Labor Life Insurance Company (Union Labor Life) discovered that an employee's work email account was accessed by an unauthorized external user. Union Labor Life issues medical stop loss coverage to the Fund. A closer review of those emails and attachments revealed that your personal information, specifically your name, SSN and personal health information, including claim numbers, dates of service, diagnosis codes and claim payments were accessible in an attachment, and may have been viewed by the unauthorized user.

Attribution 1 Publication: company release / CA AG's office / hhs. Author:
Article Title: Union Labor Life Insurance Company
Article URL: https://oag.ca.gov/system/files/SoCal%20Soft%20Drinks%20Notification%20Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171030-01	Chiorini, Hunt & Jacobs	CA	10/27/2017	Electronic	Business	Yes - Unknown #	Unknown

On September 27, 2017, we became aware that some clients received an e-mail that appeared to be from David Jacobs, but it was not. In some cases this could have included a copy of a tax return which involves your full name, birthdate, telephone number(s), address, Social Security number, or W-2s, 1099s and various other tax related documents, and direct deposit bank account information including routing numbers and account numbers if provided to us.

Attribution 1 Publication: CA AG's office Author:
Article Title: Chiorini, Hunt & Jacobs
Article URL: https://oag.ca.gov/system/files/CHJ%20Notification%20Letter%20FINAL_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171025-07	Lighthouse Management Services, LLC dba Home	NY	10/20/2017	Electronic	Business	Yes - Unknown #	Unknown

On or about July 19, 2017, Home Properties learned of suspicious activity related to an employee' s email account. On or around September 26, 2017, Home Properties determined that the affected email
account contained, and the unauthorized individual may have had access to, the following information related to you: name, address, telephone number, email address, date of birth, Social Security number, driver's license number or state identification card number, bank account number, and/or credit card number.

Attribution 1 Publication: NH AG's office / MT AG's office / NY AG' Author:
Article Title: Lighthouse Management Services, LLC dba Home Properties
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/lighthouse-management-20171020.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171025-06	Iowa Department of Human Services	IA	10/20/2017	Electronic	Government/Military	Yes - Published #	820

fficials with the Iowa Department of Human Services say the state agency was the target of a phishing email campaign last August that resulted in nine DHS employees providing their passwords which gave the hackers access to their email accounts. The campaign was discovered the same day the phishing email was sent, and DHS employees changed their passwords to block access to their email accounts and to minimize the potential for confidential information to be exposed, the department said in a news release, however the hackers potentially accessed Protected Health Information for 820 individuals during the timeframe before passwords were changed.

Attribution 1 Publication: qctimes.com / hhs.gov Author:
Article Title: Iowa Department of Human Services
Article URL: http://qctimes.com/news/state-and-regional/iowa/iowa-capitol-digest-dhs-experiences-data-breach/article_6dc798b6-3

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171025-05	Pediatric Healthcare Solutions, a Division of	NY	10/25/2017	Electronic	Medical/Healthcare	Yes - Published #	6,932

On May 22, 2017, we discovered that an unauthorized third party accessed a single computer server used to store information for patients of Pediatric Healthcare Solutions of Glen Cove, New York, a division of ProHEALTH. The information contained on the server may have included the following data: name, date of birth (DOB), Social Security number, medical ID number, address, appointment reminders, doctors' notes, vaccination reminders, clinical summaries and medical ID cards.

Attribution 1 Publication: hhs.gov / NY AG's office Author:
Article Title: Pediatric Healthcare Solutions, a Division of ProHEALTH
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171025-04	Madison Street Provider Network	CO	10/25/2017	Paper Data	Medical/Healthcare	Yes - Published #	9,129

Madison Street Provider Network CO Business Associate 9129 04/12/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Madison Street Provider Network
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171025-03	Lifestyle Therapy & Coaching	AL	10/9/2017	Electronic	Medical/Healthcare	Yes - Published #	550

Lifestyle Therapy & Coaching AL Healthcare Provider 550 10/09/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Lifestyle Therapy & Coaching
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171025-02	Orthopedics NY, LLP	NY	10/12/2017	Electronic	Medical/Healthcare	Yes - Published #	2,493

Orthopedics NY, LLP NY Healthcare Provider 2493 10/12/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Orthopedics NY, 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
ITRC20171025-01	Tarte Cosmetics	NY	10/24/2017	Electronic	Business	Yes - Unknown #	Unknown

Tarte Cosmetics, a cruelty-free cosmetics brand carried by major retailers like Sephora and Ulta, exposed the personal information of nearly two million customers in two unsecured online databases.

Attribution 1 Publication: gizmodo.com Author:
Article Title: Cosmetics Brand Tarte Exposed Personal Information About Nearly 2 Million Customers
Article URL: https://gizmodo.com/cosmetics-brand-tarte-exposed-personal-information-abou-1819723431

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171024-04	Neue Galerie	NY	10/10/2017	Electronic	Business	Yes - Unknown #	Unknown

Neue Galerie discovered on August 25, 2017, with the assistance of a third-party forensic investigation firm, that an unknown individual had placed malicious code on the Neue Galerie website that had the capability to allow unauthorized access by the individual to credit card information. As part of the ongoing investigation, Neue Galerie determined on September 7, 2017, that the following information was contained in the database: credit or debit card number, expiration date, and name.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Neue Galerie
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/neue-galerie-20171005.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171024-03	McNair & Company, Inc.	VA	10/5/2017	Electronic	Business	Yes - Unknown #	Unknown

On August 17, 2017, phishing emails were sent from the email account of a McNair employee without his knowledge. We immediately engaged a professional review firm, conducted a thorough review of the employee's email account, and determined that the account may have contained emails with your personal information, including your name and «variable data»

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: https://www.doj.nh.gov/consumer/security-breaches/documents/mcnair-20171005.pdf
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/mcnair-20171005.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171024-02	College of the Holy Cross	MA	10/23/2017	Electronic	Educational	Yes - Unknown #	Unknown

On September 22nd, 2017, a Col!ege employee accidentally cross-mailed promissory notes of at least 4, and as many as 28 College alumni via the United States Postal Service (1 of those being a resident of
New Hampshire). Due to the age of the promissory notes, they contained the names and Social Security numbers, and in some cases, Drivers License numbers of the individuals.

Attribution 1 Publication: NH AG's office Author:
Article Title: College of the Holy Cross
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/college-holy-cross-20171018.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171024-01	**coincafe**	NY	10/6/2017	Electronic	Business	Yes - Published #	**1,069**

On September 29,2017 we learned that the third party had contacted some of our customers claiming to have access to their personal information and requesting payment to erase their information. Our investigation determined that the third party had access to some customer personal information provided to us from the company's inception in January 2014 through April 11, 2014. Information in our possession at that time, including customers' names, addresses, and ID documents (driver's license, passport or other uploaded information) may have been accessed.

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: coincafe
Article URL: https://dojmt.gov/wp-content/uploads/Coincafe.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171023-04	**Carolina Oncology Specialists**	NC	10/20/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,551**

We want to make you aware of a situation we are working with local authorities to investigate. We received several credit card applications addressed to three of our patients with our street mailing address. We are aware of one patient receiving additional false inquiries.

Attribution 1 Publication: databreaches.net / company website Author:
Article Title: Carolina Oncology Specialists notifies 1,551 patients of possible breach
Article URL: https://www.databreaches.net/carolina-oncology-specialists-notifies-1551-patients-of-possible-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171023-03	**Universal Nutrition**	NJ	10/16/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On September 28, 2017, Universal Nutrition learned that unknown perpetrator(s) gained unauthorized access to its company websites, www.animalpak.com and www.universalusa.com (collectively, the “Websites”), which is suspected to have occurred in early May 2017 (the “Incident”). It appears that the unknown perpetrator(s) accessed customer information from Universal Nutrition’s Websites, including first and last name, mailing address, email address, and payment card information, including credit/debit card number, expiration date, and security verification number (collectively, “Personal Information”).

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171023-02	**Phillips & Temro Industries**	MN	10/11/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Attackers used malware to infiltrate PTI's systems, and the attack resulted in certain data being removed from PTI's systems between March and July 2017. We are not able to determine definitively what information was removed from our systems, but it is possible that the attackers removed personally identifiable information about you, including your name, address, and social security number.

Attribution 1 Publication: MT AG's office Author:
Article Title: Phillips & Temro Industries
Article URL: https://dojmt.gov/wp-content/uploads/Phillips-Temro-Industries.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171023-01	**Palomar Health**	CA	10/20/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

I regret to inform you that on September 27, 2017, an employee of Palomar Health unintentionally misdirected an email containing a worklist which included certain patient-related information about you to an unintended recipient. The email did however, contain the following types of information about you which may have been viewed: patient name, hospital-assigned identification number, admittance and discharge date, site of care (including facility and unit location), information related to coding and primary payer/health plan name.

Attribution 1 Publication: CA AG's office Author:
Article Title: Palomar Health
Article URL: https://oag.ca.gov/system/files/Palomar%20patient%20notification%20letter%20102017_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171020-01	Lincare Holdings, Inc.	FL	10/19/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A class action lawsuit claims that thousands of employees of a home healthcare services firm were harmed by the disclosure of their personal information in a breach earlier this year involving a business email compromise scam. The lawsuit alleges that the Lincare HR employee, "rather than confirming or authenticating the validity of the request, compiled the requested information and complied with the request by emailing the name, address, Social Security number, earnings information and more of current and former Lincare employees to the purported Lincare executive."

Attribution 1 Publication: healthcareinfosecurity.com Author: Marianne Kolbasuk M
Article Title: Employees Sue Home Health Provider After Phishing Breach
Article URL: https://www.healthcareinfosecurity.com/employees-sue-home-health-provider-after-phishing-breach-a-10391

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171019-01	Mann-Grandstaff VA Medical Center #2	WA	10/18/2017	Electronic	Government/Military	Yes - Published #	1,915

"Two USB hard drives containing personally-identifiable Veteran information were stolen from a Veterans Health Administration contract employee in Oklahoma on July 18, 2017. The Mann-Grandstaff VA Medical Center in Spokane has notified 1915 Veterans whose information might have been compromised. The information at risk could include full names, social security numbers, addresses, phone contacts, and surgical and insurance information.

Attribution 1 Publication: kxly.com / hipaajournal.com Author:
Article Title: Data breach at Spokane VA Medical Center
Article URL: http://www.kxly.com/news/local-news/data-breach-at-spokane-va-medical-center/640560121

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-17	ShopRite Pharmacy	CT	10/13/2017	Electronic	Medical/Healthcare	Yes - Published #	12,172

More than 7,000 people who used the pharmacy at ShopRite on Miron Lane during a recent 10-year span have been alerted by mail about a security breach that might have exposed their personal and medical information, a company spokeswoman said Friday. “The device captured customer information including name, phone number, date of birth, prescription number, medication name, date and time of pick-up or delivery, signature and ZIP code. These affected customers have been notified via letter.” Number of records per hhs.gov

Attribution 1 Publication: dailyfreeman.com / OR AG's office / NH Author:
Article Title: Ulster ShopRite breach might have exposed info about thousands of pharmacy customers
Article URL: http://www.dailyfreeman.com/general-news/20171013/ulster-shoprite-breach-might-have-exposed-info-about-thousand

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-16	Citizens Financial Group (10/4)	RI	10/4/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Our investigation into the incident determined that ATM skimming took place at a Citizens Bank ATM located in Cambridge, Massachusetts. The skimming events took place on various dates on September 6-7, 2017 and were discovered by Citizens on September 15, 2017. Customer name, debit card number, and PIN were compromised as a result of this incident.

Attribution 1 Publication: NH AG's office Author:
Article Title: Citizens Financial Group (10/4)
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-group-20171004.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-15	Nussbaum Yates Berg Klein & Wolpow	NY	10/3/2017	Electronic	Business	Yes - Published #	80,000

Recently, we learned that an unauthorized party gained access to the e-mail account of one of our partners. The e-mail account contained over 80,000 e-mails, some of which included names, Social Security numbers, drivers’ license numbers and/or financial account numbers of certain individuals. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office Author:
Article Title: Nussbaum Yates Berg Klein & Wolpow
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Nussbaum%20Yates%20Berg%20Klein%20&%20Wolp

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-14	Aegis Living	WA	10/5/2017	Electronic	Business	Yes - Unknown #	Unknown

On August 22, 2017, Aegis discovered that the email accounts of two Aegis employees were accessed by a malicious actor. The following information may have been affected: names and Social Security numbers.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-13	Aptos (August 2017) - Multiple entities	GA	10/11/2017	Electronic	Business	Yes - Unknown #	Unknown

Aptos notified us on August 25, 2017 that unauthorized third parties gained access to its systems, and that this security incident lasted from July 21, 2017 to August 9, 2017. The intrusion resulted in access to the following information: name, postal address, email address, and payment card data including credit card number, expiration date, and card verification numbers.

Attribution 1 Publication: MT AG's office / NH AG's office / VT AG' Author:
Article Title: via Atlantic Cigar Company letter / Century Martial Arts / Plow Hearth / Nutrex Hawaii / Alphaindustries.com
Article URL: https://dojmt.gov/wp-content/uploads/Atlantic-Cigar-Company.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-12	Lake Champlain Chocolates	VT	10/5/2017	Electronic	Business	Yes - Unknown #	Unknown

Lake Champlain Chocolates was made aware on September 15th, 2017 by our web hosting provider that our website had been accessed by an unauthorized party. This data may have included your name, address, email address and credit or debit card information.

Attribution 1 Publication: MT AG's office / NH AG's office / NY AG' Author:
Article Title: Lake Champlain Chocolates
Article URL: https://dojmt.gov/wp-content/uploads/Lake-Champlain-Chocolates.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-11	We Heart It	CA	10/17/2017	Electronic	Business	Yes - Unknown #	Unknown

The company was alerted to a possible security breach last week that involved over 8 million accounts, it said on Friday. The breach took place a few years ago and includes email addresses, usernames and encrypted passwords for We Heart It accounts created between 2008 and November 2013.

Attribution 1 Publication: techcrunch.com Author:
Article Title: We Heart It says a data breach affected over 8 million accounts, included emails and passwords
Article URL: https://techcrunch.com/2017/10/16/we-heart-it-says-a-data-breach-affected-over-8-million-accounts-included-emails-an

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-10	Bassett Family Practice	VA	10/17/2017	Electronic	Medical/Healthcare	Yes - Published #	500

The patient information included each person's full name, date of birth, account number at the medical practice, identity of their insurance provider and potentially some details about the reasons behind recent visits to Bassett Family Practice, such as the type of sickness a patient was suffering from. All of that information was stored on a laptop, which was sitting in an employee's car

Attribution 1 Publication: databreaches.net / MartinsvilleBulletin.c Author:
Article Title: Thieves steal Bassett facility's patient information
Article URL: http://www.martinsvillebulletin.com/news/thieves-steal-bassett-facility-s-patient-information/article_40b8c47c-b2d9-11

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-09	**Patient Home Monitoring Corp.**	LA	10/12/2017	Electronic	Medical/Healthcare	Yes - Published #	**150,000**

Another publicly accessible Amazon S3 repository has been once again been left exposing sensitive consumer information, this time affecting approximately 150,000 U.S. patients. Kromtech Security Researchers discovered the exposed server belonging to Patient Home Monitoring Corp. which contained in 47.5 GB worth of data in the form of 316,363 PDF reports detailing weekly blood test results including patient and doctor names, case management notes, other client information and the Development Server Backup, according to an Oct. 10 Mac Keeper blog post.

Attribution 1 Publication: scmagazine.com / hipaajournal.com Author:
Article Title: Another AWS leak exposes 150,000 Patient Home Monitoring Corp. client records
Article URL: https://www.scmagazine.com/patient-home-monitoring-corp-exposed-475-gb-worth-of-patient-data/article/699640/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-08	**Droege Computing Services / StampAuctionNetwork**	NC	9/26/2017	Electronic	Business	Yes - Unknown #	**Unknown**

The breach was made through our main offices and they were able access SAN from there. Based on our review of the systems, we have discovered that some of your personal data may have been compromised. This data includes your name and payment card information.

Attribution 1 Publication: CA AG's office / MT AG's office / NY AG' Author:
Article Title: Droege Computing Services / StampAuctionNetwork
Article URL: https://oag.ca.gov/system/files/DROEGE%20redacted_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-07	**Community Family Care Medical Group IPA, Inc.**	CA	10/13/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

CFC has recently become aware that one or more of our contracted Provider's, possibly including your primary care provider Roy Medical Group (Dr.s Ahdoot, Amor-Roy, Antonio, Kankar, Faustina, Shamsa, Sirajullah, Uy and Wilson), may have provided a limited amount of CFC member information to individuals working for or on behalf of the Heritage Provider Network or one of its affiliates,

Attribution 1 Publication: CA AG's office Author:
Article Title: Community Family Care Medical Group IPA, Inc.
Article URL: https://oag.ca.gov/system/files/Breach%20Letter%20-%20Clean09132017_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-05	**Transamerica / Transamerica Life Insurance Co. /**	IA	8/29/2017	Electronic	Business	Yes - Unknown #	**Unknown**

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

Attribution 1 Publication: CA AG's office / OR AG's office Author:
Article Title: Transamerica / Transamerica Life Insurance Co. / Transamerica Retirement Solutions
Article URL: https://oag.ca.gov/system/files/Individual%20Notice%20Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-04	**Pizza Hut**	TX	10/14/2017	Electronic	Business	Yes - Published #	**60,000**

The "temporary security intrusion" lasted for about 28 hours, the notice said, and it's believed that names, billing ZIP codes, delivery addresses, email addresses and payment card information — meaning account number, expiration date and CVV number — were compromised.

Attribution 1 Publication: CA AG's office / sacbee.com / NH AG's Author:
Article Title: Pizza Hut
Article URL: http://www.sacbee.com/latest-news/article178930896.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-03	**Chase Brexton Health Care**	MD	10/3/2017	Electronic	Medical/Healthcare	Yes - Published #	**16,562**

Between August 2, 2017, and August 3, 2017, a number of Chase Brexton employees received a bogus employee survey via email. It was determined that these email boxes did contain personal health information from several patients, including the following: patient name, patient ID number, date of birth, address, provider name, diagnosis codes, line of service, service location, visit description, insurance, and medication information.

Attribution 1 Publication: hhs.gov / databreaches.net / hipaajourna Author:
Article Title: Chase Brexton Health Care notifies more than 16,000 patients after phishing incident
Article URL: https://www.databreaches.net/chase-brexton-health-care-notifies-more-than-16000-patients-after-phishing-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-02	**RiverMend Health, LLC**	GA	10/9/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,300**

RiverMend launched an investigation and determined that an unauthorized individual had gained access to the employee's email account beginning on or about July 27, 2017, and continuing until August 11, 2017. This information includes the following types of patient information: name, address, age or date of birth, RiverMend facility, referral source, services rendered, and diagnostic, demographic, insurance, and/or billing information.

Attribution 1 Publication: hhs.gov / databreaches.net / MT AG's of Author:
Article Title: RiverMend Health notifies 1,300 after employee's email account compromised
Article URL: https://www.databreaches.net/rivermend-health-notifies-1300-after-employees-email-account-compromised/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171018-01	**Namaste Health Care (Bridget P. Early, MD)**	RI	10/12/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,600**

Namaste Health Care in Ashland is notifying about 1,600 patients its office experienced a security incident over the weekend of Aug. 12-13. According to a press release from office officials, the cyber attacker launched a ransomware virus/attack on the file share server, which resulted in the encryption of data housed on that server as of Aug. 14.

Attribution 1 Publication: hhs.gov / Newstribune.com Author:
Article Title: Security breach reported at Ashland clinic
Article URL: http://www.newstribune.com/news/local/story/2017/oct/14/security-breach-reported-at-ashland-clinic/695646/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171016-05	**CVS Pharmacy**	RI	10/13/2017	Paper Data	Medical/Healthcare	Yes - Published #	**836**

CVS Pharmacy RI Healthcare Provider 836 10/13/2017 Theft Paper/Films

Attribution 1 Publication: hhs.com Author:
Article Title: CVS Pharmacy
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=4D05CEF9FB5510806CD978A6F1A83B4C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171016-04	**Amida Care**	NY	9/29/2017	Paper Data	Medical/Healthcare	Yes - Published #	**6,231**

However, due to fault with the envelope printer, and in order to make sure individuals received the flyer in time, the decision was made to send out the flyer in windowed envelopes. Amida has informed all patients who received the mailing of the potential disclosure of sensitive information, which was limited to the above words

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Amida Care Mailing Potentially Revealed HIV Status of its Members
Article URL: https://www.hipaajournal.com/amida-care-mailing-potentially-revealed-hiv-status-members/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171016-02	John Hancock Life Insurance Company	MA	10/6/2017	Electronic	Business	Yes - Published #	1,715

John Hancock Life Insurance Company (U.S.A.) MA Health Plan 1715 10/06/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: John Hancock Life Insurance Company
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=4D05CEF9FB5510806CD978A6F1A83B4C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171016-01	Advanced Spine & Pain Center	TX	9/27/2017	Electronic	Medical/Healthcare	Yes - Published #	8,362

ASPC began investigating a possible security incident on July 31, 2017 after learning that some patients were being contacted and asked to pay an outstanding balance by an unknown person. As part of its investigation, ASPC discovered that its server was accessed by one or more unauthorized users. Information potentially affected by this incident includes demographic information to include name, address, Social Security Number, date of birth, state, zip code, telephone, and gender; medical information to include medical records, labs, x-rays, and scheduling notes; and billing information to include primary insurance, CPT codes, phone, ID number, and Group number.

Attribution 1 Publication: hhs.gov / databreaches.net / hipaajourna Author:
Article Title: Advanced Spine & Pain Center Notifies 8,362 Patients After Two Possibly Unrelated Incidents
Article URL: https://www.databreaches.net/advanced-spine-pain-center-notifies-8362-patients-after-two-possibly-unrelated-incident

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171011-02	TargetSmart / Equals3	AK	9/14/2017	Electronic	Business	Yes - Unknown #	Unknown

The records, totaling 593,328 individual sets of records, appear to contain every registered voter in the state of Alaska, according to security researchers at the Kromtech Security Research Center, who found the database. Each XML-formatted record contained details, some sensitive and personally identifiable information, on prospective voters, including names, addresses, dates of birth, their ethnic identity, whether an individual is married, and the individual's voting preferences.

Attribution 1 Publication: zdnet.com Author:
Article Title: Yet another trove of sensitive US voter records has leaked
Article URL: http://www.zdnet.com/google-amp/article/yet-another-trove-of-sensitive-of-us-voter-records-has-leaked/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171011-01	SVR Tracking	CA	9/21/2017	Electronic	Business	Yes - Unknown #	Unknown

The Kromtech Security Center recently found over half a million records belonging to SVR Tracking, a company that specializes in “vehicle recovery,” publicly accessible online. It contained information on roughly 540,000 SVR accounts, including email addresses and passwords, as well as some license plates and vehicle identification numbers (VIN). There were half a million records overall, Kromtech said, “but in some cases credentials were given for a record with several vehicles associated with it.”

Attribution 1 Publication: gizmodo.com Author:
Article Title: Passwords to Over a Half Million Car Tracking Devices Leaked Online
Article URL: https://gizmodo.com/passwords-to-access-over-a-half-million-car-tracking-de-1818624272

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-24	Department of Human Services, Commonwealth of	PA	9/7/2017	Electronic	Government/Military	Yes - Published #	517

Department of Human Services, Commonwealth of Pennsylvania PA Health Plan 517 09/07/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Department of Human Services, Commonwealth of Pennsylvania
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-23	Patients Choice	TX	9/26/2017	Electronic	Medical/Healthcare	Yes - Published #	1,069

Patients Choice TX Healthcare Provider 1069 09/26/2017 Hacking/IT Incident Network Server

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-22	Houston Methodist Hospital	TX	9/25/2017	Electronic	Medical/Healthcare	Yes - Published #	1,359

Houston Methodist Hospital TX Healthcare Provider 1359 09/25/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Houston Methodist Hospital
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=F24BA866202D60DA4A2783D230C3AF21

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-21	Riaz Baber, MD, S.C.	IL	9/28/2017	Paper Data	Medical/Healthcare	Yes - Published #	10,500

The medical files of more than 10,000 patients of a Naperville, IL-based psychiatrist – Dr. Riaz Baber, M.D. – have been discovered in the basement of an Aurora property by the woman who rented the house from the psychiatrist. She told reporters boxes of files were stored in the basement and that the files “has [patients] name, their address, their birthdate, their social security number, what’s wrong with them, what they’re being treated for, and what medication.”

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: PHI of 10,500 Patients of an Illinois Psychiatrist Exposed
Article URL: https://www.hipaajournal.com/phi-10500-patients-illinois-psychiatrist-exposed/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-20	T-Mobile (INCD2017-08-3628325)	WA	9/14/2017	Electronic	Business	Yes - Unknown #	Unknown

As part of an internal investigation, we have determined that your credit card number ending in XXXX was misused by a former employee of T-Mobile

Attribution 1 Publication: NH AG's office Author:
Article Title: T-Mobile (INCD2017-08-3628325)
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/t-mobile-20170914.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-19	PerfectServe, Inc.	TN	9/27/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

At this time, PerfectServe does not know for certain that its systems or vendors were the source of such compromise. However, out of an abundance of caution, PerfectServe is providing notice and identity theft protection services to those potentially affected. The IRS has informed PerfectServe that individual names, dates of birth, addresses, and social security numbers are required in order to obtain the IRS documents in question.

Attribution 1 Publication: NH AG's office Author:
Article Title: PerfectServe, Inc.
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/perfectserve-20170927.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-18	**Lendio**	UT	9/15/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

Lendio was caught in a “phishing” attack on or about the last week of May 2017. This information included your name, address, date of birth, Social Security number, the payment information you provided in conjunction with your franchise purchase application, and some business-related information including Federal Employer Identification Number, address, and other business contact information.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Lendio
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/lendio-20170915.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-17	**Gentle Giant Studios, Inc. dba Gentle Giant, Ltd.**	CA	9/26/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Gentle Giant observed that an unauthorized JavaScript link had been introduced to the "footer" of its ecommerce website. cript link had been introduced to the "footer" of its ecommerce website. The exfiltrated data included names, addresses, telephone numbers, email addresses and payment card numbers, expiration dates and CVV numbers of customers who provided new or updated payment information on Gentle Giant's ecommerce website between April 24, 2017 and August 4, 2017.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Gentle Giant Studios, Inc. dba Gentle Giant, Ltd.
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/gentle-giant-studios-20170926.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-16	**Denver Art Museum**	CO	10/4/2017	Electronic	Business	Yes - Published #	**821**

Specifically, on or about September 13, 2017, the Museum discovered that certain of its email accounts may have been compromised by an unknown actor. In particular, the compromise was a result of malicious email received by the Museum, which allowed access to personal information about a limited number of donors, customers, and employees.

Attribution 1 Publication: NH AG's office / Denverpost.com / NY A Author:
Article Title: Denver Art Museum
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/denver-art-20171003.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-15	**Citizens Financial Group, Inc. (10/4)**	RI	10/4/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

The skimming events took place on various dates on September 6-7, 2017 and were discovered by Citizens on September 15, 2017. Customer name, debit card number, and PIN were compromised as a result of this incident.

Attribution 1 Publication: NH AG's office Author:
Article Title: Citizens Financial Group, Inc. (10/4)
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-group-20171004.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-14	**Rudy Cecchi & Associates / Valmark Financial Group**	FL	9/21/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On July 31 , 2017, we learned that an unauthorized person gained access to email accounts beginning on July 28, 2017. We conducted a thorough review of the email accounts and determined that it contained your first and last name, address, Social Security number, driver's license number, and health insurance and/or medical information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Rudy Cecchi & Associates / Valmark Financial Group
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/cecchi-20170920.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-13	**AM2 / Approve.Me**	UT	9/20/2017	Electronic	Business	Yes - Published #	**13,088**

On or around July 31, 2017, the Company learned that an error in the Approve.Me 1 software caused an inadvertent disclosure of information pertaining to a subset of its customers. The personal information shared with the second lender includes customers' names and Social Security numbers.

Attribution 1 Publication: NH AG's office / VT AG's office / NY AG' Author:
Article Title: AM2 / Approve.Me
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/am2-20170919.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-12	**Kenco Group**	TN	10/2/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On August 30, 2017, a member of the Kenco Wellness Team accidentally emailed a spreadsheet containing confidential information about associates when providing a status update regarding the associates who had and had not registered for our BRAVO screenings. The spreadsheet attached to the email included personal information such as names, phone numbers, dates of birth, email addresses, and Social Security numbers.

Attribution 1 Publication: OR AG's office / NY AG's office Author:
Article Title: Kenco Group
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1967723867

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-11	**Brown/Armstrong, PC**	OR	9/21/2017	Electronic	Business	Yes - Published #	**1,003**

On September 5, 2017, based on discussions with the IRS/CI, we determined that client information may have been accessed without authorization. he following information may have been affected: tax return information which included names, addresses, dates of birth, Social Security numbers and bank account numbers.

Attribution 1 Publication: OR AG's office / NY AG's office Author:
Article Title: Brown/Armstrong, PC
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/2090054119

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-10	**Briggs & Stratton**	WI	9/29/2017	Electronic	Business	Yes - Published #	**33,000**

We value and respect the privacy of information which is why Briggs & Stratton Corporation (Briggs) is writing to follow up with you and your health plan dependents and insurance beneficiaries regarding a recent malware attack on Briggs' computer systems at its Milwaukee, Wisconsin and Munnsville, New York locations that potentially compromised information from approximately July 25, 2017 to July 28, 2017. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office / hhs.go Author:
Article Title: Briggs & Stratton
Article URL: https://dojmt.gov/wp-content/uploads/Briggs-Stratton.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-09	**Cheddar's Scratch Kitchen**	TX	9/29/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Early on July 21, 2017, there was a break-in at locked corporate facility for Cheddar's Scratch Kitchen in Texas that resulted in the theft of several laptops and a hard drive containing some team members' personal information and very limited guest information. While the investigation continues, our current understanding is that the personal information that may have been involved in the incident likely includes your Social Security number; contact information, such as your name, address, email address, and telephone number; other employment-related information and limited guest information, if applicable. In some cases, a photocopy of your ID may have been included. We regret that your personal information may be affected.

Attribution 1 Publication: MT AG's office / NH AG's office / CA AG' Author:
Article Title: Cheddar's Scratch Kitchen
Article URL: https://dojmt.gov/wp-content/uploads/Cheddars-Casual-Cafe.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-08	**626498 Alberta Ltd. / Best Western Plus**	AZ	9/18/2017	Electronic	Business	Yes - Published #	**262**

On July 20, 2017, the forensic investigator confirmed that one of our reservation system computers was infected with a form of malware that collected certain payment information entered into the reservation system or swiped at the front desk. The data elements potentially subject to unauthorized access include your: name, address, phone number, email address as well as your credit card number and expiration date. In addition, if your card was swiped at the front desk your CVV code
was also affected.

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: Best Western Plus
Article URL: https://dojmt.gov/wp-content/uploads/Best-Western-Plus-Wine-Country-Hotel.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-07	**Northwestern Mutual Life Insurance Company**	WI	8/31/2017	Electronic	Business	Yes - Unknown #	**Unknown**

During the course of a telephone call, fraudsters used social engineering methods to gain remote access to my desktop computer on August 31, 2017, and several times thereafter. Some of your personally identifiable information may have been compromised, such as your name, date of birth, social security number, health/medical information, policy/account information and banking information.

Attribution 1 Publication: CA AG's office Author:
Article Title: Northwestern Mutual Life Insurance Company
Article URL: https://oag.ca.gov/system/files/%20Sample%20Client%20Notification%20Letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-06	**FlexShopper, LLC**	NC	10/3/2017	Electronic	Business	Yes - Published #	**170,474**

On August 30, 2017, FlexShopper discovered that a database containing customer information may have been inadvertently accessible on the internet for a few days. The investigation determined that customer names, email addresses, passwords, addresses, phone numbers, dates of birth, Social Security numbers, employment information, self-reported income, bank account information and/or payment card information were potentially exposed. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / VT AG' Author:
Article Title: FlexShopper, LLC
Article URL: https://oag.ca.gov/system/files/FlexShopper%20-%20AG%20Notice%20-%20CA_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-05	**Cabrillo Community College**	CA	9/4/2017	Electronic	Educational	Yes - Published #	**12,273**

On September 5, 2017, we learned that an unauthorized person gained accessed to one of our servers. The student orientation information included your name, date of birth, Social Security number, email address, user name, and password used to access the online orientation module at www.sirena.cabrillo.edu. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / databreaches.net / kion Author:
Article Title: Cabrillo Community College
Article URL: http://www.kion546.com/news/cabrillo-college-issues-notice-of-data-breach-to-28000-students/632786868

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-04	**SyncHR - multiple**	CO	10/6/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On August 23. 2017. SyncHR became aware that a report containing your benetits that was intended to be accessed solely by your employer in our production environment was temporarily accessable by HR
administrators of other customers. Your personal infonnation, including your name. address. date of birth. social security number, employment information (e.g., employer name, hiring date), and benefits selection information as well as in some cases the name, address, date of birth and social security number of your dependents, was possibly accessed.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: SyncHR - multiple
Article URL: https://oag.ca.gov/system/files/SyncHR%20Breach%20-%20Sample%20Notification%20Ltr%20%28CA%29_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-03	**Tommie Copper**	NY	8/29/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On August 24, 2017, the forensic investigator confirmed that a piece of malware had been inserted into our website at checkout that this malware from our checkout site.The data elements potentially subject to unauthorized access include your: name, address, phone number, email address and credit and/or debit card information.

Attribution 1 Publication: CA AG's office / OR AG's office / MT AG Author:
Article Title: Tommie Copper
Article URL: https://oag.ca.gov/system/files/Tommie%20Copper%20-%20Notice%20of%20Data%20Event%20-%20CA%20-%20Exhibi

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-02	**Catholic United Financial**	MN	10/6/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**127,310**

On September 20, 2017, the forensic investigator issued its final report which concluded that Catholic United Financial's web server had been subjected to SQL injection attacks by an unknown person(s). We estimate that approximately 127,310 current and former members, whose on-file addresses indicate they live in a variety of locations including in your state, may have had their personal information containing Social Security numbers accessed, including approximately 7,356 deceased members.

Attribution 1 Publication: CA AG's office / TwinCities.com / MT A Author:
Article Title: Data breach at Arden Hills-based Catholic financial services provider affects nearly 130K accounts
Article URL: https://oag.ca.gov/system/files/Catholic%20United%20Financial%20Template%20Consumer%20Notice_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171010-01	**Provo Craft & Novelty, Inc. dba Cricut**	UT	10/5/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We have learned that the checkout page on a prior version of our website was the subject of a cyberattack, which was designed to scrape payment and personal information of customers at checkout while making purchases. The payment card number, security code and expiration date as well as names, addresses and contact information.

Attribution 1 Publication: CA AG's office / MT AG's office / VT AG' Author:
Article Title: Kayser-Roth Corporation / Hue
Article URL: https://oag.ca.gov/system/files/Provo%20Craft%20Consumer%20Notification%20Letter_2.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-33	**Drexel University**	PA	9/25/2017	Electronic	Educational	Yes - Published #	**299**

After an email from Student Disability Services on Sept. 6 accidentally revealed the email addresses of 299 students who receive accommodations, Drexel University Law professor Robert Field said Penn will likely receive a "slap on the wrist" in terms of legal repercussions.

Attribution 1 Publication: databreaches.net / thedp.com Author:
Article Title: A legal expert weighs in on Student Disability Services' accidental leak of 299 emails
Article URL: http://www.thedp.com/article/2017/09/a-legal-experts-weighs-in-on-student-disability-services-accidental-leak-of-299-e

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-32	**Auburn Eyecare Associations (TDO)**	CA	9/26/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

TDO had first informed DataBreaches.net of this particular hack back in June, and had provided some sample patient data, a portion of which appears below as redacted by this site. The patient records included patients' names, dates of birth, Social Security numbers, postal addresses and telephone numbers, all in plain text. For some patients, e-mail addresses were also included:

Attribution 1 Publication: databreaches.net Author:
Article Title: Auburn Eye Care Associates: Can you see it NOW?
Article URL: https://www.databreaches.net/auburn-eye-care-associates-can-you-see-it-now/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-31	San Ysidro School District	CA	9/28/2017	Electronic	Educational	Yes - Unknown #	Unknown

Malware infected computers at a local school district this month, deleting emails and forcing the district to temporarily shut down part of its systems.

Attribution 1 Publication: databreaches.net / inewsource.org Author:
Article Title: Malware attacks San Ysidro School District, demands $19K ransom
Article URL: https://inewsource.org/2017/09/28/malware-san-ysidro-ransom/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-30	North Carolina A&T State University	NC	9/28/2017	Electronic	Educational	Yes - Published #	1,581

The personal information of 1,581 students at North Carolina A&T State University was leaked following a “data security incident.” It happened on Tuesday when a faculty member within the College of Business and Economics accidentally emailed a file containing personal information to a group of students. The data included banner identifications, birthdates, GPA’s, addresses, phone numbers and email addresses.

Attribution 1 Publication: databreaches.net / myfox8.com Author:
Article Title: Some NC A&T students’ personal information leaked in ‘security incident’
Article URL: http://myfox8.com/2017/09/28/some-nc-at-students-personal-information-leaked-in-security-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-29	National Football League	NY	10/3/2017	Electronic	Business	Yes - Published #	1,133

The personal data of more than 1,100 NFL players and agents was exposed as the result of a misconfigured online database, a cybersecurity company has revealed.

Attribution 1 Publication: thehill.com Author:
Article Title: Private data of more than 1,100 NFL players, agents exposed
Article URL: http://thehill.com/policy/cybersecurity/353664-private-data-of-more-than-1100-nfl-players-agents-exposed

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-28	Whatcom Land Title Company	WA	9/16/2017	Electronic	Banking/Credit/Financial	Yes - Published #	433

Whatcom Land Title Company (WLT) learned August 4, 2017 that it was the target of a phishing scam. The type of information available in the account includes: customer names, mailing addresses, email addresses, phone numbers, social security numbers, drivers license numbers, passports, loan numbers, and bank account numbers.

Attribution 1 Publication: WA AG's office Author:
Article Title: Whatcom Land Title Company
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/WhatcomLandTitle

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-27	Green River College	WA	8/24/2017	Electronic	Educational	Yes - Published #	3,399

We discovered on 15 August 2017 that GRC employee personal information was compromised. The compromised information includes employee names and Social Security numbers.

Attribution 1 Publication: WA AG's office Author:
Article Title: Green River College
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/GreenRiverCommu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-26	Richard E. Munoz, CPA	CA	9/20/2017	Electronic	Business	Yes - Unknown #	Unknown

On August 24, 2017, I became aware that some of you had received an e-mail that appeared to be from me, but it was not. The information may have included correspondence with your Social Security number.

Attribution 1 Publication: MT AG's office Author:
Article Title: Richard E. Munoz, CPA
Article URL: https://dojmt.gov/wp-content/uploads/Richard-Munoz-CPA.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-25	CliftonLarsonAllen LLP	MN	9/20/2017	Electronic	Business	Yes - Published #	1,239

On August 28, 2017, CLA discovered a third-party service provider's client portal system had been compromised via a user's login credentials, permitting unauthorized access to certain client information. The following information may have been obtained by unauthorized individual(s): tax and wage information, names, addresses, dates of birth, Social Security numbers and bank account numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / VT AG's office / NH AG' Author:
Article Title: CliftonLarsonAllen LLP
Article URL: https://dojmt.gov/wp-content/uploads/Clifton-Larson-Allen.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-24	NCI Group, Inc.	TX	9/22/2017	Electronic	Business	Yes - Unknown #	Unknown

On August 8, 2017, we learned that an unknown individual was able to access three employees' email accounts. While there is no indication that the unknown individual was able to access any other email accounts or systems beyond these three email accounts, the investigation determined that some of our customers' information was contained in the accounts, including your name and Social Security number.

Attribution 1 Publication: MT AG's office / NH AG's office / NY AG' Author:
Article Title: NCI Group, Inc.
Article URL: https://dojmt.gov/wp-content/uploads/NCI-Group.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-23	Aero-Tech Light Bulb Co.	IL	9/22/2017	Electronic	Business	Yes - Published #	802

On July 6, 2017, Aero-Tech learned that a company server had been infected with ransomware despite the company's data security protections. Aero-Tech discovered on September 6, 2017, that some personal information may have been accessible, including some customer's name, address, payment card number, expiration date and security code (CVV).

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: Aero-Tech Light Bulb Co.
Article URL: https://dojmt.gov/wp-content/uploads/Aero-Tech-Light-Bulb-Co.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-22	Securities Exchange Commission	DC	10/2/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

On 20 September, Clayton revealed that the infiltration of the Edgar system - which houses non-public filings on upcoming corporate earnings statements and pending mergers and acquisitions - was detected in 2016 but that the watchdog only realised in August that data stolen may have been used for illicit trading.

Attribution 1 Publication: finextra.com Author:
Article Title: SEC data breach: hackers accessed personal information
Article URL: https://www.finextra.com/newsarticle/31137/sec-data-breach-hackers-accessed-personal-information

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-21	Iowa Lottery	IA	9/26/2017	Electronic	Business	Yes - Published #	3,000

The Iowa Lottery will offer credit monitoring to nearly 3,000 lottery winners after their Social Security numbers were mistakenly posted on a website, lottery officials said Tuesday.

Attribution 1 Publication: desmoinesregister.com Author:
Article Title: Iowa Lottery accidentally releases Social Security numbers for 3,000 winners
Article URL: http://www.desmoinesregister.com/story/news/2017/09/26/Iowa-lottery-says-personal-data-winners-inadvertently-relea

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-20	Deloitte	NY	9/25/2017	Electronic	Business	Yes - Unknown #	Unknown

Deloitte, one of the world's "big four" accounting firms, has acknowledged a breach of its internal email systems, British news outlet The Guardian revealed today. In a story published Monday morning, The Guardian said a breach at Deloitte involved usernames, passwords and personal data on the accountancy's top blue-chip clients.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Source: Deloitte Breach Affected All Company Email, Admin Accounts
Article URL: https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-19	Sonic Drive-In	OK	9/28/2017	Electronic	Business	Yes - Published #	5,000,000

On Wednesday, a data breach at drive-in food chain Sonic jeopardized the security of credit cards from up to 5 million customers, whose accounts are being "peddled in shadowy underground cybercrime stores," website Krebs on Security informed.

Attribution 1 Publication: newsweek.com / CA AG's office / MT A Author:
Article Title: SONIC'S DATA BREACH: WHY ARE CREDIT CARDS STILL GETTING HACKED?
Article URL: http://www.newsweek.com/sonics-data-breach-why-are-credit-cards-still-getting-hacked-672962

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-18	Whole Foods	TX	9/30/2017	Electronic	Business	Yes - Unknown #	Unknown

Whole Foods officials said the credit and debit card information of customers who bought meals or drinks at its in-store restaurants or bars were exposed to hackers.

Attribution 1 Publication: wavy.com / WI AG's office / CA AG's offi Author:
Article Title: Whole Foods warns shoppers of a data breach
Article URL: http://wavy.com/2017/09/30/whole-foods-warns-shoppers-of-a-data-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-17	Gratan Resort & Casino	CA	9/30/2017	Electronic	Business	Yes - Unknown #	Unknown

An undisclosed number of patrons at Graton Resort and Casino are being notified by mail of what casino officials said was an inadvertent email distribution of personal information such as names, addresses and Social Security numbers of patrons.

Attribution 1 Publication: pressdemocrat.com Author:
Article Title: Graton casino 'data breach' potentially reveals some patrons' Social Security numbers
Article URL: http://www.pressdemocrat.com/news/7478449-181/graton-casino-data-breach-potentially?artslide=0

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-16	SMART Physical Therapy	MA	9/26/2017	Electronic	Medical/Healthcare	Yes - Published #	16,428

The hack reportedly occurred on September 13, 2017, with the announcement of the data theft disclosed by TDO on Twitter on Friday 22, 2017. The database contained a wide range of information on 16,428 patients, including contact information, dates of birth and Social Security numbers.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Another Healthcare Organization Attacked by The Dark Overlord
Article URL: https://www.hipaajournal.com/healthcare-hack-the-dark-overlord/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-15	Hyatt Centric The Loop Chicago / Integrated Clark	IL	8/7/2017	Electronic	Business	Yes - Published #	24,599

Guest payment card information for guests who used payment cards at check-in from September 27, 2016 to April 28, 2017 may have been compromised and may have been used for an unauthorized purpose. An unauthorized person installed malware on the Hotel's front desk computer system designed to capture credit and debit card information. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NY AG's office Author:
Article Title: Integrated Clark Monroe, LLC / Hyatt Centric The Loop Chicago
Article URL: https://oag.ca.gov/system/files/IHR%20HYATT%20CENTRIC%20LOOP%20CA%20NOTIFICATION%20FINAL%20%28J22

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-13	Indiana Health Centers, Inc.	IN	9/12/2017	Electronic	Medical/Healthcare	Yes - Published #	1,697

Indiana Health Centers, Inc. IN Healthcare Provider 1697 09/12/2017 Theft Desktop Computer, Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Indiana Health Centers, 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
ITRC20171003-12	Stephen P. Courtney, MD	TX	10/3/2017	Electronic	Medical/Healthcare	Yes - Published #	1,140

Stephen P. Courtney, M.D. TX Healthcare Provider 1140 03/01/2017 Unauthorized Access/Disclosure Electronic Medical Record, Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Stephen P. Courtney, 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
ITRC20171003-11	Urological Associates of Central Jersey P.A.	NJ	9/18/2017	Electronic	Medical/Healthcare	Yes - Published #	1,800

Urological Associates of Central Jersey P.A. NJ Healthcare Provider 1800 09/18/2017 Hacking/IT Incident Desktop Computer, Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Urological Associates of Central Jersey 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
ITRC20171003-10	Mann-Grandstaff VA Medical Center #1	WA	9/20/2017	Electronic	Government/Military	Yes - Published #	3,275

A decommissioned laptop computer previously used by the Mann-Grandstaff VA Medical Center (MGVAMC) in Spokane, WA, has been discovered to be missing, potentially resulting in the exposure of sensitive patient data. The types of information stored on the device would have included names, dates of birth, and Social Security numbers according to a statement issued by MGVAMC.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Lost Laptop Sees PHI of 3,725 Veterans Exposed
Article URL: https://www.hipaajournal.com/lost-laptop-sees-phi-3725-veterans-exposed/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-09	**Network Health**	WI	9/8/2017	Electronic	Medical/Healthcare	Yes - Published #	**51,232**

In August 2017, some Network Health employees received sophisticated phishing emails. The compromised email accounts contained a range of sensitive information including names, phone numbers, addresses, dates of birth, ID numbers, and provider information.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Network Health Phishing Attack Impacts 51,000 Plan Members
Article URL: https://www.hipaajournal.com/network-health-phishing-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-08	**MN Urology**	MN	9/18/2017	Electronic	Medical/Healthcare	Yes - Published #	**939**

MN Urology MN Healthcare Provider 939 09/18/2017 Unauthorized Access/Disclosure Email

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-07	**Our Lady of the Angels Hospital / Formerly Bogalusa**	LA	9/22/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,200**

Our Lady of the Angels Hospital has discovered a former employee accessed the medical records of 1,140 patients without authorization. The types of information accessed by the former employee includes names, addresses, phone numbers, dates of birth, gender, insurance information, social security numbers, diagnoses, dates of services, places of services, and clinical information such as orders, test results, medications, and clinical abstracts.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Our Lady of the Angels Hospital Breach Impacts 1,140 Patients
Article URL: https://www.hipaajournal.com/our-lady-of-the-angels-hospital-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-06	**Mercy Health / Love County Hospital and Clinic**	OK	9/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	**13,004**

On June 23, 2017, the hospital discovered an employee had stolen a laptop computer and paper records from a storage unit used by the hospital.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: 13,000 Patients Potentially Impacted by Mercy Health Love County Hospital Breach
Article URL: https://www.hipaajournal.com/13000-mercy-health-love-county-hospital-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-05	**August University Medical Center**	GA	9/15/2017	Electronic	Medical/Healthcare	Yes - Published #	**6,109**

AU Medical Center, Inc. GA Healthcare Provider 6109 09/15/2017 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
Article Title: August University 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
ITRC20171003-04	**Kraig R. Pepper. D.O, P.A.**	TX	9/26/2017	Electronic	Medical/Healthcare	Yes - Published #	**653**

Kraig R. Pepper, D.O., P.A. TX Healthcare Provider 653 09/26/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Kraig R. Pepper. D.O, 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
ITRC20171003-03	Arkansas Oral & Facial Surgery Center	AR	9/24/2017	Electronic	Medical/Healthcare	Yes - Published #	128,000

Arkansas Oral & Facial Surgery Center AR Healthcare Provider 128000 09/24/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov / hipaajournal.com / scmagazin Author:
Article Title: Ransomware Attack Potentially Impacts 128,000 Arkansas Patients
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-02	International Council of Shopping Centers	NY	8/8/2017	Electronic	Business	Yes - Unknown #	Unknown

On August 18, 2017, we received a report regarding payment card activity that caused us to investigate and subsequently identify unauthorized computer code that was added to the code that operates the checkout page of www.icsc.org. The information on the checkout page that the code could have potentially accessed includes name, address, phone number, email address, payment card number, expiration date, and card security code (CVV).

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: International Council of Shopping Centers
Article URL: https://oag.ca.gov/system/files/International%20Council%20of%20Shopping%20Centers%20Ad%20CA_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171003-01	Online Traffic School	CA	9/29/2017	Electronic	Business	Yes - Unknown #	Unknown

On July 26, 2017, we discovered that an unauthorized individual gained access to part of our computer network that supports the applications and websites that we operate. Based on the investigation, we believe that the unauthorized individual may have been able to acquire your name, address, email address, and payment card number and expiration date.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Online Traffic School
Article URL: https://oag.ca.gov/system/files/Combined%20CA_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20171002-01	Servis One, Inc. dba BSI Financial Services	TX	9/25/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

An unauthorized third-party illegally gained access to one of our employees e-mail accounts on or about June 1, 2017.This information may have included borrower names and addresses, account numbers, and other account information

Attribution 1 Publication: CA AG's office Author:
Article Title: Servis One, Inc. dba BSI Financial Services
Article URL: https://oag.ca.gov/ecrime/databreach/reports/sb24-102180

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-20	Premier Medical Associates	PA	9/15/2017	Electronic	Medical/Healthcare	Yes - Published #	876

Monroeville-based Premier Medical Associates, owned by Highmark Health, Friday reported a data breach involving 900 patients and visitors to its website. Website visitors who submitted information through the “Contact us” portion of Premier Medical Associates' website may have been exposed to the breach. “PMA's investigation also found that several public search engines, including Google and Bing, crawled PMA's website as part of their routine activities and retrieved the visitors' submissions,” a news release said.

Attribution 1 Publication: databreaches.net / triblive.com / hhs.gov Author:
Article Title: Highmark affiliate Premier Medical Associates reports data breach
Article URL: http://triblive.com/news/healthnow/12739457-74/monroeville-medical-practice-reports-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-19	Medical Mutual of Ohio	OH	9/19/2017	Electronic	Medical/Healthcare	Yes - Published #	6,119

Medical Mutual of Ohio (Medical Mutual) is taking action after recently discovering that an email containing personal information belonging to a portion of its Medicare Advantage members was inadvertently sent to an incorrect email address.

Attribution 1 Publication: databreaches.net / northwestsignal.net Author:
Article Title: Medical Mutual Provides Notice of Data Incident
Article URL: http://www.northwestsignal.net/news/health/article_5a5d307e-03cc-524a-97a0-9686c926fd88.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-18	Fiduciary Management, Inc.	WI	9/6/2017	Electronic	Banking/Credit/Financial	Yes - Published #	3,287

On August 7, 2017, we discovered that the email account of one of our employees had been subject to unauthorized access earlier that day. While our investigation is ongoing, your name, or your organization or trust's name, your Social Security number or Taxpayer Identification number, and the custodial bank or brokerage account number that FMI manages or managed on your behalf, may have been present in the impacted email account. (Exposure number per NY Ag's office)

Attribution 1 Publication: MT AG's office / NH AG's office / MD AG Author:
Article Title: Fiduciary Management, Inc.
Article URL: https://dojmt.gov/wp-content/uploads/Fiduciary-Management.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-17	reThink Group, Inc.	NY	9/6/2017	Electronic	Business	Yes - Unknown #	Unknown

On July 11, a network intruder uploaded malicious code to our operating system which allowed the intruder to obtain access to certain personal information provided by customers on our websites. The incident involved customer names, addresses, credit card numbers, CVV#s, and expiration dates.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-16	Jacuzzi	CA	9/11/2017	Electronic	Business	Yes - Unknown #	Unknown

Jacuzzi Brands LLC's (and some of its subsidiaries based in the United States) payroll vendor, Ceridian, recently became aware of an issue that may affect you. On September 1, Ceridian inadvertently emailed password protected files containing your personal information to another Ceridian customer. Based on the investigation, it has been determined that the files included information such as first and last name, address, phone number, social security number, bank account information, and payroll information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-15	Frontier Cooperative	IA	9/11/2017	Electronic	Business	Yes - Unknown #	Unknown

In August we confirmed that a data security incident could have impacted some visitors to ourwebsites who placed orders between Friday, May 12, 2017 and Tuesday, August 22, 2017. While the investigation is still ongoing, we have confirmed the possibility that unauthorized individuals may have gained access to your name, the shipping and billing address, and the payment card number used to make your purchase on one of our sites.

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: Frontier Cooperative
Article URL: https://dojmt.gov/wp-content/uploads/Frontier-Natural-Products.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-14	Signator Investors, Inc.	NH	9/11/2017	Electronic	Business	Yes - Unknown #	Unknown

On August 23, 2017, Signator determined that an unknown third party had gained unauthorized access to certain client records, some as early as June 2017. The information that the perpetrator may have viewed or acquired includes your name, address, date of birth, social security number, telephone number, email address, product account numbers, and balances of your accounts with us.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-13	E & J Gallo Winery	CA	9/15/2017	Electronic	Business	Yes - Published #	7,730

On August 30, 2017, Gallo learned that a former employee recently obtained employee data without authorization. he following personal information may have been involved: names, Social Security numbers and financial account information. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / CA AG's office / NY AG' Author:
Article Title: E & J Gallo Winery
Article URL: https://dojmt.gov/wp-content/uploads/E-J-Gallo-Winery.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-12	PeaceHealth Southwest Medical Center	WA	9/18/2017	Electronic	Medical/Healthcare	Yes - Published #	1,969

Nearly 2,000 patients at PeaceHealth Southwest Medical Center are being notified that an employee unnecessarily accessed their private health information. The Vancouver medical center discovered on Aug. 9 that the employee accessed electronic files containing protected health information, including patient names, ages, medical record and account numbers, admission and discharge dates, progress notes and diagnosis.

Attribution 1 Publication: MT AG's office / databreaches.net / colu Author:
Article Title: PeaceHealth employee accessed patient info unnecessarily
Article URL: http://www.columbian.com/news/2017/sep/15/peacehealth-employee-accessed-patient-info-unnecessarily/?utm_conte

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-11	Grainger	CA	9/20/2017	Electronic	Business	Yes - Published #	1,594

On August 23, 2017, Grainger learned that a team member's laptop was stolen. The information may have included data such as the following: name, contact information, including home address, Social Security number, date of birth, and employee benefits information. Each individual may have been affected differently.

Attribution 1 Publication: OR AG's office / MT AG's office / CA AG Author:
Article Title: Grainger
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/510023946

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-10	ICC Industries, Inc.	NY	9/7/2017	Electronic	Business	Yes - Published #	4,997

On or around July 24, 2017, ICC received reports of suspicious activity that affected users' ability to access certain data and systems. This activity included the disabling of ICC user accounts and the deletion of files. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-09	**Arkansas Department of Human Services / Medicaid**	AR	9/18/2017	Electronic	Government/Military	Yes - Published #	**26,044**

A former employee of the Arkansas Department of Human Services (DHS) has been fired from her new position at the state hospital for emailing spreadsheets containing the protected health information of patients to a personal email account. The spreadsheets were found to contain a range of sensitive information of patients including names, birth dates, linked Medicaid identification numbers, diagnoses, codes for medical procedures, and some Social Security numbers.

Attribution 1
Publication: hipaajournal.com Author:
Article Title: Hospital Employee Fired Over 26,000-Record Arkansas DHS Privacy Breach
Article URL: https://www.hipaajournal.com/hospital-employee-fired-over-26000-record-arkansas-dhs-privacy-breach-8969/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-08	**Morehead Memorial Hospital**	NC	9/18/2017	Electronic	Medical/Healthcare	Yes - Published #	**66,000**

Morehead Memorial Hospital in Eden, NC has announced two employees have fallen victim to a phishing attack that resulted in an unauthorized individual gaining access to their email accounts. The types of information exposed includes names, health insurance payment summaries, health insurance information, treatment overviews, and a limited number of Social Security numbers.

Attribution 1
Publication: hipaajournal.com / MT AG's office / hhs. Author:
Article Title: Phishing Attack Results in the Exposure of PHI at Morehead Memorial Hospital
Article URL: https://www.hipaajournal.com/phishing-attack-results-in-the-exposure-of-phi-at-morehead-memorial-hospital-8970/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-07	**Cohn Handler Sturm**	CA	9/11/2017	Electronic	Business	Yes - Published #	**2,192**

On July 29, 2017, a partner's pin protected cell phone was stolen from his person. Potentially any emails and attachments exchanged with asturm@cohnhandler.com. This information may have included a financial account number provided to Cohn Handler Sturm.

Attribution 1
Publication: CA AG's office / NY AG's office Author:
Article Title: Cohn Handler Sturm
Article URL: https://oag.ca.gov/system/files/CHS%20Notification_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-06	**Ridgeview Medical Center**	MN	9/8/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,074**

According to Ridgeview, on July 10 and 11, Ridgeview Community Network sent a general survey request to network members. The survey was sent to a group of people via email – which visibly included email address and was not blind-copied, and allowed all recipients of the survey to see the email addresses of other recipients.

Attribution 1
Publication: hhs.gov / databreaches.net / Laker & Pio Author:
Article Title: Ridgeview Medical Center
Article URL: http://lakerpioneer.com/2017/09/17/data-breach-made-public-ridgeview-says-it-exposed-some-email-addresses/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-05	**Barer Law Offices**	MT	9/5/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On Tuesday May 23,2017, my law office was the subject of a burglary in which a computerwas stolen. You may wish to take action to determine if any personal information has been accessed by an unauthorized person or otherwise used by an unauthorized person.

Attribution 1
Publication: Barer Law Offices Author:
Article Title: Barer Law Offices
Article URL: https://dojmt.gov/wp-content/uploads/Barer-Law-Offices.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-04	**Med-Cert, Inc.**	FL	9/2/2017	Electronic	Medical/Healthcare	Yes - Published #	**7,253**

On July 7, 2017, Med-Cert, Inc., a pre-certification and utilization review service provider for employer group health plans, learned that an unauthorized person accessed the network of Med-Cert's website host and accessed and disclosed certain personal information. The following personal or protected health information of you, your minor dependent, or your loved one may have been impacted: name, birthdate, employer, Social Security number, and medical information (name of health care provider, treatment and diagnosis information, and insurance policy information).

Attribution 1 Publication: hhs.gov / company press release / ME A Author:
Article Title: Med-Cert, Inc.
Article URL: http://www.businesswire.com/news/home/20171018006635/en/Med-Cert-Data-Breach-Notice

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-03	**MS Center of Saint Louis and Mercy Clinic Neurology -**	MO	9/16/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,081**

1,081 patients of the MS Center of Saint Louis and Mercy Clinic Neurology Town and Country are being informed that they may be contacted for marketing and research purposes by pharmaceutical companies and other third-parties, even though they may not have given their permission to be contacted. Protected health information detailed on the forms includes names, email addresses, telephone numbers, home addresses, health insurance information, and in some cases, treatment and prescription information and Social Security numbers.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: 1,081 St. Louis Patients Alerted About Improper PHI Disclosure
Article URL: https://www.hipaajournal.com/1081-st-louis-patients-alerted-improper-phi-disclosure-8975/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-02	**Florida Healthy Kids Corporation**	FL	9/7/2017	Electronic	Medical/Healthcare	Yes - Published #	**2,000**

On July 25, 2017, phishing emails started to arrive in the inboxes of members of staff, some of whom responded and inadvertently gave the attackers access to the sensitive information of members of the KidCare program. The types of information exposed includes names, addresses, phone numbers, family account numbers, and Social Security numbers.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Florida Healthy Kids Corporation Announces 2,000 Patients' Impacted by Phishing Scam
Article URL: https://www.hipaajournal.com/florida-healthy-kids-corporation-announces-2000-patients-impacted-phishing-scam-897

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170921-01	**Consultants Choice**	FL	9/1/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,458**

Consultants Choice, P.A. FL Healthcare Provider 1458 09/01/2017 Hacking/IT Incident Desktop Computer

Attribution 1 Publication: hhs.gov Author:
Article Title: Consultants Choice
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=091AD8DECFAC11C9805C3B9C35F66B47

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-19	**C. Jerry Ploss & Co.**	NY	9/12/2017	Electronic	Business	Yes - Published #	**334**

Description of breach: A breach occurred on 1/2/17 but was only first discovered on 2/2/17. It was an external breach (ie hack) of our network. It appears that an external agent was able to access our 2015 tax preparation software.Types of information believed to be accessed: Name, address, social security numbers, 2015 tax return information. (Exposure number per NY AG's office)

Attribution 1 Publication: CT AG's office / NY AG's office Author:
Article Title: C. Jerry Ploss & Co.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-18	Adveq Management US, Inc.	NY	9/12/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Upon learning of the incident, Adveq US conducted an internal investigation and determined that on February 10, 2017, the 2016 W-2 forms of Adveq US employees and several former employees of Adveq US were provided to an unknown and unauthorized person outside of the Adveq organization through an email phishing scam. The information compromised consists of the information found on W-2 forms, including the individual's full name, address and Social Security number, 2016 compensation amount, and amounts deducted from his compensation, as applicable, for federal, state, and local taxes, 401(k)and flexible spending.

Attribution 1 Publication: CT AG's office / NY AG's office Author:
Article Title: Adveq Management US, Inc.
Article URL: Per FOIA CT AG's office / Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-17	Nationwide	OH	9/12/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 15, we determined that an associate may have downloaded files containing your personal information. The information the associate may have downloaded includes your name and social security number.

Attribution 1 Publication: Per FOIA CT AG's office / Per FOIL NY Author:
Article Title: Nationwide
Article URL: Per FOIA CT AG's office / Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-16	Santander Bank (3/24)	MA	9/12/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 24, 2017, the Santander Bank Physical Security Command Center performed a video review of the ATM located at 1290 Avenue of the Americas, New York, NY, and identified that a deep insert skimming device had been placed on the ATM on January 8, 2017 and removed January 9, 2017. 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: CT AG's office Author:
Article Title: Santander Bank (3/24)
Article URL: Per FOIA CT AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-15	Santander Bank (3/8)	MA	9/12/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 8, 2017, Santander Bank Fraud Risk Management discovered suspicious ATM withdrawals. 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: CT AG's office Author:
Article Title: Santander Bank (3/8)
Article URL: Per FOIA CT AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-14	Cooper's Hawk Winery & Restaurants	IL	9/12/2017	Electronic	Business	Yes - Unknown #	Unknown

On or about February 21, 2017, we became aware of the potential unauthorized access of certain e-mails and attachments from approximately January 8, 2017 to February 21, 2017. During the relevant period, those e-mails and attachments contained your personal information including your name, Social Security number and/or driver's license.

Attribution 1 Publication: CT AG's office / NY AG's office Author:
Article Title: Cooper's Hawk Winery & Restaurants
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-13	Clark Rasmussen Taylor, CPAs	UT	9/12/2017	Electronic	Business	Yes - Published #	1,361

On April II, 2017, Clark Rasmussen Taylor, CPAs ("CRTCPAs") discovered a data incident which may have resulted in unauthorized access or acquisition of your personal information as the result of a ransomware attack. The data elements involved may have included name, address, birth date, Social Security number, and financial information.

Attribution 1 Publication: CT AG's office Author:
Article Title: Clark Rasmussen Taylor, CPAs
Article URL: Per FOIA CT AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-12	Harvey Mudd College	CA	9/12/2017	Electronic	Educational	Yes - Published #	170

On February, 2017, we learned that an unauthorized individual may have gained access to an employee's email account. We conducted a thorough review of the employee's e-mail account and confirmed that a message contained your name and social security number. (Exposure number per NY AG's office)

Attribution 1 Publication: AG's office / NY AG's office Author:
Article Title: Harvey Mudd College
Article URL: Per FOIA CT AG's office / Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-11	Little River Waco Ear, Nose & Throat	TX	8/28/2017	Electronic	Medical/Healthcare	Yes - Published #	500

On June 26, 2017, it was discovered that Little River Waco Ear Nose and Throat was the victim of a ransomware attack that encrypted the data stored on some of our computers and servers. The records that potentially have been impacted may include your name, address, date of birth, Social Security number, and medical information.

Attribution 1 Publication: hhs.gov / MT AG's office Author:
Article Title: Waco Otolaryngology Associates dba Waco Ear, Nose & Throat
Article URL: https://dojmt.gov/wp-content/uploads/Little-River-Healthcare.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-10	MetroPlus Health Plan, Inc.	NY	9/1/2017	Electronic	Medical/Healthcare	Yes - Published #	15,212

On July 6, 2017, we discovered that a limited amount of your personal information was contained in MetroPlus emails sent by a staff member to an unauthorized recipient. The information that was potentially involved includes the following: • Demographic Information {Name, Date of Birth, Member ID, Gender, Race/Ethnicity), Health Insurance Claim umber/SSN, Umited Diagnostic Information, and Primary Care Physician name and address.

Attribution 1 Publication: hhs.gov / NY AG's office Author:
Article Title: MetroPlus Health Plan, Inc.
Article URL: Per FOIA Request NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-09	Velcro USA Inc. / ADP	NH	8/31/2017	Electronic	Business	Yes - Unknown #	Unknown

On August 24, 2017, the company became aware of suspicious changes in the self-service portal of the ADP system which the company uses for payroll processing. It was determined however, that electronic bank account information, pay information, and in some cases social security information was accessed by the persons responsible for the breach. Our investigation has also revealed that the individuals who had their direct deposit information changed in the ADP system had been targets of a phishing attack which occurred on August 17, 2017.

Attribution 1 Publication: NH AG's office Author:
Article Title: Velcro USA Inc.
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/velcro-20170901.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-08	SRI International	CA	9/7/2017	Electronic	Business	Yes - Unknown #	Unknown

In late July 2017, SRI discovered that internal SRI networks and systems were targeted and improperly accessed by unauthorized parties. After extensive investigation, SRI has determined that the categories of personal information that may have been accessed include your name, address, email address, telephone, Social Security number, taxpayer identification number, wage and tax information, date of birth, and direct deposit information.

Attribution 1
Publication: NH AG's office / VT AG's office / MT AG' Author:
Article Title: SRI International
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/sri-20170907.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-07	reThink Group, Inc.	GA	9/6/2017	Electronic	Business	Yes - Unknown #	Unknown

On July 11, a network intruder uploaded malicious code to our operating system which allowed the intruder to obtain access to certain personal information provided by customers on our websites. The incident involved customer names, addresses, credit card numbers, CVV#s, and expiration dates.

Attribution 1
Publication: NH AG's office Author:
Article Title: The reThink Group, Inc.
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/rethink-group-20170907.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-06	New York Life Insurance Company	NY	9/5/2017	Electronic	Business	Yes - Published #	243

On August 21, 2017, an unauthorized individual who had obtained an agent's personal information including social security number impersonated the agent to gain access to some of the agent's client information. New York Life determined that the unauthorized individual accessed the personal information of 1 New Hampshire resident, including their name, dates of birth, last 4 digits of their social security number, and policy numbers. (Exposure number per NY AG's office)

Attribution 1
Publication: NY AG's office Author:
Article Title: New York Life Insurance Company
Article URL: Per FOIL NY AG's office

Attribution 2
Publication: NH AG's office / NY AG's office Author:
Article Title: New York Life Insurance Company
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/new-york-life-20170905.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-05	Infinite Computer Solutions, Inc.	MD	9/1/2017	Electronic	Business	Yes - Published #	650

Infinite recently discovered that one of our test servers, which contained information of some of our employees for testing purposes, was compromised on or around May 26, 2017 by an unauthorized party. At this time, we believe the files at issue may have included human resources and employment related information, such as your name, date of birth, social security number, driver's license number, passport number, financial account information, Alien Registration number, and other employment-related documentation, including, if applicable, 1-9 forms, W4 forms, direct deposit forms, life insurance forms, beneficiary forms, background investigation forms, drug testing forms, personnel action forms, emergency contact forms, and/or offer letters. (Exposure number per NY AG's office)

Attribution 1
Publication: NH AG's office / NY AG's office Author:
Article Title: Infinite Computer Solutions, Inc.
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/infinite-computer-solutions-20170901.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-04	Kroeschell, Inc.	IL	8/31/2017	Electronic	Business	Yes - Published #	1,543

On June 30, 2017, the third-party forensic investigators identified malware on our system with keylogging capabilities, and have more recently determined that the malware potentially had the ability to allow someone to see or download data. While these investigations are ongoing, we determined on July 25, 2017 that the following information about you may have been accessible to the unauthorized individual: Social Security number, financial account number, user names and passwords and/or security questions entered onto your workcomputer, and name. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-03	WRJ Holdings, LLC dba Classic Firearms	NC	9/1/2017	Electronic	Business	Yes - Unknown #	Unknown

Forensic analysis determined on August 14 that a malicious attacker could modify a legitimate file to obtain access to our server, enabling the attacker to compile payment card information into a file. The following personal information may have been accessed during the incident: first and last names, address(es), phone numbers, credit card numbers, credit card expiration dates, credit card identification numbers, and dates of birth.

Attribution 1 Publication: MT AG's office / NH AG's office / ME AG Author:
Article Title: WRJ Holdings, LLC dba Classic Firearms
Article URL: https://dojmt.gov/wp-content/uploads/Classic-Firearms.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-02	Akira / shopakira.com	IL	9/1/2017	Electronic	Business	Yes - Published #	22,513

On July 18, 2017, the forensic investigator confirmed that our website was infected with a form of malicious code that collected certain payment information used at checkout. The data elements potentially subject to unauthorized access include your: name, address, phone number, email address and credit and/or debit card information.

Attribution 1 Publication: MT AG's office / NH AG's office / / NY A Author:
Article Title: Akira / shopakira.com
Article URL: https://dojmt.gov/wp-content/uploads/Akira.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170912-01	ABB, Inc.	NC	8/25/2017	Electronic	Business	Yes - Published #	28,012

ABB, Inc. (“ABB”), received notice on August 25, 2017, that an employee’s email account had suspicious login activity as the result of a hacker sending a phishing scheme email to ABB employees on or around August 25, 2017. The compromised email account(s) may have stored your personal information, including your name, address social security number and medical record(s) used in ABB Employee Benefits, FMLA, and in some instances direct deposit information for a few number of hourly staff located in one selected location. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / hhs.gov / MT AG's offic Author:
Article Title: ABB, Inc.
Article URL: https://oag.ca.gov/system/files/ABB%20Sample%20Notification%20Letter%20to%20Individuals_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170911-07	Timberland Bank	WA	7/31/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On July 18, 2017, Timberland learned that courier bags containing loan files and paper checks processed by Timberland had been stolen from the company that provides Timberland’s courier services during transit between Timberland branches. The following types of personal information may have been contained in the loan files and on the checks: name, address, date of birth, Social Security number, driver’s license information, telephone number, bank account information, routing number, and other documentation typically collected during the loan application process.

Attribution 1 Publication: WA AG's office Author:
Article Title: Timberland Bank
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/TimberlandBank.20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170911-06	Oncology Consultants, PA	TX	8/22/2017	Electronic	Medical/Healthcare	Yes - Published #	19,114

On June 19. 21117, Oncology Consultants learned it was the victim of a cyber attack that included ransomware, which encrypted the data stored on some of its computer servers. The information the attackers may have had access to includes patient demographics such as names, date of birth, Social Security numbers, home addresses. email addresses, employment information, as well as medical information including health care ID numbers. test results. and diagnostic codes.

Attribution 1 Publication: hhs.gov / NY AG's office Author:
Article Title: Oncology Consultants, PA
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170911-05	Mercy Hospital Logan County	OK	8/30/2017	Paper Data	Medical/Healthcare	Yes - Published #	629

Mercy Hospital Logan County OK Healthcare Provider 629 08/30/2017 Loss Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Mercy Hospital Logan County
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170911-04	Adult Internal Medicine of North Scottsdale (TDO)	AZ	9/1/2017	Electronic	Medical/Healthcare	Yes - Published #	11,798

Adult Internal Medicine of North Scottsdale AZ Healthcare Provider 11798 09/01/2017 Hacking/IT Incident Network Server (TDO)

Attribution 1 Publication: hhs.gov Author:
Article Title: Adult Internal Medicine of North Scottsdale
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170911-03	Community Memorial Health System	CA	9/7/2017	Electronic	Medical/Healthcare	Yes - Published #	959

The protected health information of almost 1,000 patients has potentially been accessed as a result of a recent Community Memorial Health System phishing attack. The email account was discovered to contain a selection of protected health information including patients' names, medical record numbers, dates of services, and a limited amount of health information

Attribution 1 Publication: hipaajournal.com / hhs / CA AG's office Author:
Article Title: Community Memorial Health System Phishing Attack Reported
Article URL: https://www.hipaajournal.com/community-memorial-health-system-phishing-attack-reported-8954/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170911-02	University of Wisconsin-Madison's Department of	WI	9/8/2017	Electronic	Medical/Healthcare	Yes - Published #	1,000

A request to take part in a survey was sent via mail, but rather than sending letters inside sealed envelopes, the decision was taken to send postcards. Printed on the postcards, in plain sight, were references to prescribed medications and family planning services: A violation of patient privacy and breach of HIPAA Rules

Attribution 1 Publication: hippajournal.com Author:
Article Title: Mailing Error and PHI Breach Underscores Need for Greater Oversight
Article URL: https://www.hipaajournal.com/mailing-error-phi-breach-underscores-need-greater-oversight-8955/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170911-01	Children's Hospital Colorado	CO	9/11/2017	Electronic	Medical/Healthcare	Yes - Published #	3,370

Almost 3,400 patients of Children's Hospital Colorado are being notified that some of their protected health information has potentially been accessed by an unauthorized individual who gained access to the email account of a staffer.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 3,400 Patients of Children's Hospital Colorado Potentially Impacted by Email Hack
Article URL: https://www.hipaajournal.com/childrens-hospital-colorado-potentially-impacted-email-hack-8959/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170907-01	Equifax	GA	9/7/2017	Electronic	Business	Yes - Published #	145,500,000

Criminal hackers gained access to files including sensitive personal data for 143 million Americans— Social Security numbers, birth dates and home addresses — by penetrating a Web-based application for Equifax, the credit reporting agency said Thursday.

Attribution 1 Publication: findbiometrics.com / NY AG's office Author:
Article Title: Breached Records Total Goes Up with Conclusion of Equifax Forensic Investigation
Article URL: https://findbiometrics.com/equifax-forensic-investigation-410033/

Attribution 2 Publication: Washington Post / CA AG's office Author: Craig Timberg and Eli
Article Title: Hackers access database that has personal data for 143 million Americans from credit reporting agency Equifax
Article URL: https://www.washingtonpost.com/news/the-switch/wp/2017/09/07/hackers-steal-personal-data-for-143-million-america

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-18	Mr. Cooper (7/5/2017)	TX	8/31/2017	Electronic	Banking/Credit/Financial	Yes - Published #	8,118

Nationstar Mortgage LLC d/b/a Mr. Cooper ("Mr. Cooper") discovered on July 5th 2017 that an incident occurred where your loan number and property address were inadvertently populated on another borrower's letter. This incident resulted in another borrower receiving your property address and loan number in their letter. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / CA AG's office / MD AG Author:
Article Title: Mr. Cooper (7/5/2017)
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/nationstar-mortgage-20170831.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-17	LPL Financial (6/17)	CA	8/14/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Regrettably, on June 8, 2017, we were notified that your advisor's office hired an employee without informing LPL Financial. As a result, your personal information, including name, LPL Financial account number and Social Security number, may have been exposed to unauthorized access.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: LPL Financial
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/lpl-financial-20170822.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-16	GT Distibutors	TX	8/25/2017	Electronic	Business	Yes - Published #	1,287

On July 28, 2017, we learned that an unauthorized third party may have obtained access to the servers that operate our e-commerce website, www.gtdist.com. The information that may have been affected includes customer's name, address, phone number, email address, payment card number, expiration date and security code (CVV). (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MT AG's office / MD AG Author:
Article Title: GT Distibutors
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/gt-distributors-20170825.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-15	Citizens financial Group (8/29)	RI	8/29/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

The skimming events took place on various dates in July and August 2017 and were discovered by Citizens on August 14, 2017. Customer name, debit card number, and PIN were compromised as a result of this incident.

Attribution 1 Publication: NH AG's office Author:
Article Title: Citizens financial Group (8/29)
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/citizens-20170829.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-14	CBS Consolidated, Inc. dba Cornerstone Business &	NE	8/23/2017	Electronic	Business	Yes - Published #	21,856

On July 10, 2017, during our routine review of our system logs, we discovered an account on our server that we did not recognize. The personal information involved included your name, address, date of birth, and insurance information, which may include a social security number if you had coverage through Medicare for the durable medical equipment and supplies.

Attribution 1 Publication: NH AG's office / MT AG's office / hipaajo Author:
Article Title: CBS Consolidated, Inc. dba Cornerstone Business & Management Solutions
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/cbs-consolidated-20170823.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-13	Mark F. Andrews, CPA, LLC	MA	8/24/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 27, 2017, I became aware that some of my clients had tax returns filed by an unknown third party. The investigation determined that your name, address, Social Security number and other tax information within my tax software may have been viewed or accessed by an unknown, unauthorized third party.

Attribution 1 Publication: NH AG's office / ME AG's office / NY AG Author:
Article Title: Mark F. Andrews, CPA, LLC
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/andrews-cpa-20170824.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-12	American Friends Service Committee	PA	8/21/2017	Electronic	Business	Yes - Unknown #	Unknown

Recall that on April18, 2017, we discovered a data incident which involved your personal information as the result of a temporary employee's unauthorized access to and procurement of the personal information of some of our employees' personal information. The elements of personal information involved in the incident included names, addresses, social security numbers, dates of birth, and salary information.

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: American Friends Service Committee
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/american-friends-20170821.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-11	City of Oceanside	CA	8/23/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

The city of Oceanside has shut down its online bill-paying system for utility customers while it investigates a possible data breach of customers' account and credit card information.

Attribution 1 Publication: CA AG's office Author:
Article Title: City of Oceanside
Article URL: https://oag.ca.gov/system/files/Notice%20of%20Data%20Breach%20%28Final%209-6-17%29_0.pdf

Attribution 2 Publication: sandiegouniontribune.com / CA AG's offi Author:
Article Title: Oceanside investigating possible data theft on bill-paying website
Article URL: http://www.sandiegouniontribune.com/communities/north-county/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-10	**Major League Lacrosse**	MA	8/28/2017	Electronic	Business	Yes - Published #	**2,570**

On Thursday, August 24, 2017, we became aware that a link on our player pool registration inadvertently linked to an Excel spreadsheet which contained your full name, address, telephone number, email address, social security number, citizenship, date of birth, height, weight, position, college, graduation year, team, and non-MLL occupation. (Exposure number per NY AG's office)

Attribution 1 Publication: uslaxmagazine.com / NH AG's office / N Author:
Article Title: Major League Lacrosse
Article URL: Per FOIA request NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-09	**CVS Caremark**	RI	8/30/2017	Electronic	Medical/Healthcare	Yes - Published #	**4,000**

CVS Caremark, a division of the CVS pharmacy and healthcare company, abruptly discontinued a mailing last week to patients in Ohio receiving HIV-related medication from the company after it learned that a reference to “HIV” appeared above the patients’ names in the window of the envelopes sent to about 4,000 people.

Attribution 1 Publication: washingtonblade.com Author:
Article Title: CVS exposes patients’ HIV status in mailings
Article URL: https://www.washingtonblade.com/2017/08/30/cvs-caremark-exposes-patients/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-08	**Hand Rehabilitation Specialists**	CA	9/1/2017	Electronic	Medical/Healthcare	Yes - Published #	**12,806**

On July 5, 2017, we were informed that there may have been a breach in the security of our network. The information may have included your: name, date of birth, address, phone number, Social Security number, dates of service, diagnoses, CPT (billing) codes, cost, amount of co-pay made by check, medical insurance company, insurance group number and contact information, check number, and our name and practice contact information. (TDO) (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NY AG's office Author:
Article Title: Hand Rehabilitation Specialists
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Hand%20&%20Upper%20Extremity%20Centers%20SB

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-07	**Spectrum / Time Warner Cable / BroadSoft**	NC	9/5/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Kromtech Security Center researchers discovered late last week that about four million Time Warner customer records were exposed when it found two cloud-based AWS S3 buckets, connected to software and service provider BroadSoft, open to the public. The information compromised spanned the period from November 10, 2010 to July 7, 2017, and included transaction numbers, MAC numbers, user names, account numbers types of service purchased along with internal development information like SQL database dumps and code with login credentials, Kromtech said.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Data breach exposes about 4 million Time Warner customer records
Article URL: https://www.scmagazine.com/data-breach-exposes-about-4-million-time-warner-customer-records/article/686592/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-06	**Kaleida Health**	NY	8/31/2017	Electronic	Medical/Healthcare	Yes - Published #	**744**

The investigation determined the unauthorized individual may have gained access to a small number of Kaleida Health email accounts, which may have included patient names, medical record numbers and diagnoses, among other information. Officials reported 744 individuals were affected in the incident, according to an Aug. 25 submission to HHS' Office for Civil Rights breach portal.

Attribution 1 Publication: beckershospitalreview.com / NY AG's off Author:
Article Title: Kaleida Health reports 2nd phishing attack in 2 months
Article URL: http://www.beckershospitalreview.com/cybersecurity/kaleida-health-reports-2nd-phishing-attack-in-2-months.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-05	**Medical Oncology Hematology Consultants**	DE	9/4/2017	Electronic	Medical/Healthcare	Yes - Published #	**19,203**

A server and several workstations used by Newark, Delaware-based Medical Oncology Hematology Consultants (MOHC) have had sensitive data encrypted by ransomware. The types of information potentially compromised were limited to patients' names, phone numbers, dates of birth, health and treatment information. In total, 19,203 patients were potentially impacted by the incident.

Attribution 1 Publication: hipaajournal.com / beckershospitalrevie Author:
Article Title: 19,000 Impacted by Medical Oncology Hematology Consultants Ransowmare Incident
Article URL: https://www.hipaajournal.com/19000-impacted-by-medical-oncology-hematology-consultants-ransowmare-incident-89

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-04	**Neurology Foundation**	RI	9/5/2017	Electronic	Medical/Healthcare	Yes - Published #	**12,861**

The Neurology Foundation discovered the employee had copied data onto the hard drive during an exit interview on May 3, 2017. The information copied to the external storage device included patients' names, addresses, phone numbers, dates of birth, email addresses, health insurance policy numbers, medical record numbers, bank account numbers, medical diagnoses, Social Security numbers, details of treatments and medications, and patients' race and sex.

Attribution 1 Publication: hipaajournal.com / MT AG's office / NH Author:
Article Title: Former Employee of The Neurology Foundation Discovered to Have Obtained Patient Data
Article URL: https://www.hipaajournal.com/former-employee-neurology-foundation-discovered-obtained-patient-data-8951/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-03	**Alaska Department of Health and Social Services**	AK	9/5/2017	Electronic	Government/Military	Yes - Published #	**501**

A Trojan horse virus has been discovered on two computers used by the Alaska Department of Health and Social Services. The virus potentially allowed malicious actors to gain access to the data stored on the devices. Those documents contained details of family case files, medical diagnoses and observations, personal information and other related information.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Alaska DHSS Discovers Malware Infection and Possible PHI Breach
Article URL: https://www.hipaajournal.com/alaska-dhss-discovers-malware-infection-and-possible-phi-breach-8952/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-02	**Kaiser Permanente - Riverside (9/2017)**	CA	8/30/2017	Electronic	Medical/Healthcare	Yes - Published #	**609**

On August 9th, 2017, a document containing your protected health information was inadvertently emailed from a Kaiser Permanente facility to an external email address. The misdirected email contained a document with the name, medical record number, procedure and date of service for a specific list of people

Attribution 1 Publication: CA AG'soffice / beckershospitalreview.c Author:
Article Title: Kaiser Permanente - Riverside
Article URL: https://oag.ca.gov/system/files/Breach%20Notification%20Letter.Final_._0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170905-01	**TigerSwan / TalentPen**	NC	9/3/2017	Electronic	Business	Yes - Published #	**9,400**

Thousands of files containing personal data on former military, intelligence and government workers have allegedly been exposed to public view for months in a massive security lapse allowed by a US-based recruitment firm. Some 9,400 sensitive files were found unsecured on a misconfigured public-facing Amazon cloud server.

Attribution 1 Publication: newsline.com Author:
Article Title: 9,400 resumes of US military & intel contractors exposed in massive security lapse – reports
Article URL: https://newsline.com/9400-resumes-of-us-military-intel-contractors-exposed-in-massive-security-lapse-reports/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-21	Piersol Construction, Inc.	WA	8/15/2017	Electronic	Business	Yes - Unknown #	Unknown

On July 19, 2017, we were alerted to irregularities in certain banking transactions. We immediately alerted our bank's personnel, who were able to determine that certain Piersol documents were stolen from the U.S. mail. The following information may have been accessed: names, addresses, dates of birth, and Social Security numbers.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-20	Evers Robinson	AZ	8/21/2017	Electronic	Business	Yes - Unknown #	Unknown

On July 17, 2017, Evers Robinson learned of a data security incident that may have affected individuals whose information was stored on the Evers Robinson ShareFile, a file sharing program provided by a third party vendor to Evers Robinson.

Attribution 1 Publication: MT AG's office / MD AG's office / NY AG Author:
Article Title: Evers Robinson
Article URL: https://dojmt.gov/wp-content/uploads/Arizona-Tile.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-19	Rutherford, MacDonald & Olson, P.C.	MT	8/23/2017	Electronic	Business	Yes - Unknown #	Unknown

Based on the results of a forensic investigation we confirmed that someone was able to gain unauthorized access to our server in March and April of 2017. The unauthorized party was able to access our server, which contains, among other things, information relating to client tax returns — including Social Security Number, name, address, telephone number, and other state and federal income tax filing related information.

Attribution 1 Publication: MT AG's office / MD AG's office / ME A Author:
Article Title: Rutherford, MacDonald & Olson, P.C.
Article URL: https://dojmt.gov/wp-content/uploads/Rutherford-MacDonald-Olson.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-18	Crescent Mortgage Company	GA	8/24/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On August 4, 2017, we learned that certain information related to customer mortgage loans was accessed without authorization by an outside third party between the dates of July 14, 2017 and August 5, 2017. As a result of this incident, an unauthorized person may have accessed some of your sensitive personal information, including your first and last name, home address, phone number, social security number, and financial accounts, as well as personal information contained within documents related to your loan application and closing documents, including wiring instructions.

Attribution 1 Publication: MT AG's office / NH AG's office / MD AG Author:
Article Title: Crescent Mortgage Company
Article URL: https://dojmt.gov/wp-content/uploads/Crescent-Mortgage-Company.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-17	City of Port Angeles	WA	7/25/2017	Electronic	Government/Military	Yes - Published #	9,400

Yesterday the City of Port Angeles received reports from customers of possible credit card compromise. Also today, letters were sent to all of the City's approximately 9,400 utility customers informing them of a possible breach. In the letter, we recommended that, as a precaution, they verify all recent credit or debit transactions.

Attribution 1 Publication: WA AG's office Author:
Article Title: City of Port Angeles
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/CityOfPortAngeles.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-16	**WellCare Health Plans, Inc.**	FL	8/11/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,214**

WellCare Health Plans, Inc. FL Health Plan 1214 08/11/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: WellCare Health Plans, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=405596A05D185E1F4E21732AC45F9C0B

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-15	**Spectrum Health System**	MI	8/3/2017	Electronic	Medical/Healthcare	Yes - Published #	**902**

Spectrum Health System MI Healthcare Provider 902 08/03/2017 Theft Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: Spectrum Health System
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=405596A05D185E1F4E21732AC45F9C0B

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-14	**South Bend Orthopaedic Associates, Inc.**	IN	8/18/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,272**

South Bend Orthopaedic Associates Inc IN Healthcare Provider 1272 08/18/2017 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: South Bend Orthopaedic Associates, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=405596A05D185E1F4E21732AC45F9C0B

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-13	**Silver Cross Hospital**	IL	8/11/2017	Electronic	Medical/Healthcare	Yes - Published #	**8,862**

Silver Cross Hospital in New Lenox, IL, has learned that the protected health information of 8,862 patients has been exposed as a result of a software update performed by a business associate that manages certain parts of its website.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Website Update Exposes PHI of 8,800 Silver Cross Hospital Patients
Article URL: http://www.hipaajournal.com/website-update-exposes-phi-8800-silver-cross-hospital-patients-8942/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-12	**Salina Family Healthcare Center**	KS	8/16/2017	Electronic	Medical/Healthcare	Yes - Published #	**77,337**

On June 18, 2017, we were the target of a ransomware attack that encrypted some of our computer workstations and network servers. Although the investigation did not identify any evidence of access to your information, we could not rule out the possibility that your personal information, including your name, address, Social Security number, date of birth, health insurance information, and medical treatment information is at risk.

Attribution 1 Publication: hhs.gov / MT AG's office / hipaajournal.c Author:
Article Title: Salina Family Healthcare Center
Article URL: https://dojmt.gov/wp-content/uploads/Salina-Family-Healthcare-Center.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-11	**Northwest Behavioral Healthcare Services**	OR	7/27/2017	Electronic	Medical/Healthcare	Yes - Published #	**500**

Northwest Behavioral Healthcare Services OR Healthcare Provider 500 07/27/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Northwest Behavioral Healthcare Services
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=405596A05D185E1F4E21732AC45F9C0B

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-10	Northeast OB/GYN Associates	TX	8/18/2017	Electronic	Medical/Healthcare	Yes - Published #	10,198

Northeast OB/GYN Associates TX Healthcare Provider 10198 08/18/2017 Hacking/IT Incident Desktop Computer, Laptop, Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Northeast OB/GYN Associates
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=405596A05D185E1F4E21732AC45F9C0B

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-09	McLaren Medical Group / Mid-Michigan Physicians Imaging	MI	8/24/2017	Electronic	Medical/Healthcare	Yes - Published #	106,008

McLaren Medical Group, which manages Mid-Michigan Physicians, has announced that the breach affected a system that stored scanned internal documents such as physician orders and scheduling information, which included protected health information such as names, addresses, telephone numbers, dates of birth, Social Security numbers, medical record numbers, and diagnoses.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: 106,000 Mid-Michigan Physicians' Patients Potentially Impacted by Breach
Article URL: https://www.hipaajournal.com/106000-mid-michigan-physicians-patients-potentially-impacted-breach-8948/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-08	Feinstein and Roe, MDs, Inc.	CA	8/21/2017	Electronic	Medical/Healthcare	Yes - Published #	6,642

Feinstein and Roe Mds Inc. CA Healthcare Provider 6642 08/21/2017 Hacking/IT Incident Network Server (TDO)

Attribution 1 Publication: hhs.gov Author:
Article Title: Feinstein and Roe, MDs, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=405596A05D185E1F4E21732AC45F9C0B

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-07	Bluetail Medical Group	MO	8/2/2017	Electronic	Medical/Healthcare	Yes - Published #	11,000

Bluetail Medical Group MO Healthcare Provider 11000 08/02/2017 Hacking/IT Incident Desktop Computer

Attribution 1 Publication: hhs.gov Author:
Article Title: Bluetail Medical Group
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=405596A05D185E1F4E21732AC45F9C0B

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-06	Aetna	CT	8/29/2017	Paper Data	Medical/Healthcare	Yes - Published #	11,887

An error was made in a recent mailing to plan members. That error resulted in the HIV positive of members being disclosed to other individuals. However, some of that information was visible through the transparent plastic window in the envelope along with names and addresses.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Third-Party Mailing Error Sees Aetna Plan Members' HIV Status Disclosed
Article URL: http://www.hipaajournal.com/third-party-mailing-error-sees-aetna-plan-members-hiv-status-disclosed-8939/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-05	**Zazzle Inc.**	CA	7/30/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We take security extremely seriously at Zazzle and wanted to let you know that in July 2017, our Security Team detected a brute force data security attack. Given the nature of the incident, Zazzle believes that your username (email address) and password may have been obtained by an unauthorized third party, through a breach of other website(s), who then tried to confirm your credentials on our site.

Attribution 1 Publication: CA AG's office Author:
Article Title: Zazzle Inc.
Article URL: https://oag.ca.gov/system/files/Zazzle%20-%20Individual%20Notice%20-%20CA_20170825_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-04	**Zymo Research Corporation**	CA	8/25/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Unfortunately, on or about August 2, 2017, Zymo Research Corporation ("Zymo") discovered that its external cloud e-commerce network may have been accessed by an unknown actor. The personal information about Zymo's customers maintained in the database affected by the unauthorized access included first and last names; physical addresses; email addresses as well as hashed passwords; and credit card information, including credit card number, card verification code, and expiration date.

Attribution 1 Publication: CA AG's office / NH Ag's office / MT AG' Author:
Article Title: Zymo Research Corporation
Article URL: https://oag.ca.gov/system/files/Zymo%20Research%20Ad%20CA-WY%20r4fin_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-03	**Franklin R. Noto, CPA**	CA	7/30/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On July 27, 2017, a burglar broke into our locked office. Upon discovery that same day, an employee immediately called the police and had the window replaced. The password protected information included your: full name, address, and Social Security number.

Attribution 1 Publication: CA AG's office Author:
Article Title: Franklin R. Noto, CPA
Article URL: https://oag.ca.gov/system/files/Noto%20Final%20letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-02	**Massachusetts Mutual Life Insurance Company**	MA	8/17/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Upon conducting an investigation into that the activity identified, it was determined that beginning on August 17, 2017 an unknown perpetrator contacted MassMutual call centers purporting to be two separate MassMutual insurance agents. Your personal information that may have been involved includes your name, Social Security number, MassMutual policy/account number, [address], [date of birth], [and telephone number].

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Massachusetts Mutual Life Insurance Company
Article URL: https://oag.ca.gov/system/files/DRAFT%20-%20General%20Client%20notification_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170830-01	**CoreLogic Credco**	CA	8/27/2017	Electronic	Business	Yes - Published #	**2,189**

Credco learned that between July 21, 2017 and August 7, 2017 an individual obtained access to Credco's system to obtain your consumer information without proper authorization. Such information includes your name and address and one or more of the following: Social Security Number, date of birth and account numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MD AG's office / NY AG Author:
Article Title: CoreLogic Credco
Article URL: https://oag.ca.gov/system/files/CA%20CLCR%20Cnsmr%20Notification%20Lttr%20-%20AllClearID%20Identity%20Prot

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-20	**Standex International Corporation**	NH	8/8/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On May 19, 2017, we learned that an unauthorized person gained access to an employee's email account beginning on April 20, 2017. Standex conducted a thorough review of the employee's email account and determined that it contained individual names, Social Security numbers, drivers' license numbers, and in some cases passport numbers.

Attribution 1 Publication: NH AG's office / ME AG's office Author:
Article Title: Standex International Corporation
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/standex-20170808.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-19	**Saddle Ridge Partners, LLC dba Wizard Labs**	FL	8/14/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We recently became concerned that an unauthorized person may have accessed our systems in an attempt to acquire confidential information. These systems process customer orders and include such information as names, addresses, payment account numbers, and/or email addresses.

Attribution 1 Publication: NH AG's office / MD AG's office / ME A Author:
Article Title: Saddle Ridge Partners, LLC dba Wizard Labs
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/saddle-ridge-20170807.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-18	**New Hampshire Retirement System**	NH	7/24/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On friday, July 21, 2017, NHRS learned that an unidentified, unauthorized party established a number of online accounts in early July in NHRS' "My Account" system, which is our web portal for retirees like you. To establish a My Account, the party who engaged in this activity entered the retiree 's last name, home zip code, date of birth, and the last four digits of his or her social security number (SSN).

Attribution 1 Publication: NH AG's office Author:
Article Title: New Hampshire Retirement System
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/new-hampshire-retirement-system-20170809.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-17	**KBE Building Corporation**	CT	8/4/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Regrettably, we are writing to inform you of a sophisticated e-mail phishing incident that occurred on July 28, 2017. The incident involved disclosure of your W-2 information, which included your name, address, Social Security number and income information.

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: KBE Building Corporation
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/kbe-building-20170804.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-15	**Elderplan, Inc.**	NY	8/5/2017	Electronic	Medical/Healthcare	Yes - Published #	**22,000**

On June 6, 2017, MJHS learned that an unauthorized individual gained access to the email accounts of several employees of Elderplan Inc., and on June 14, 2017 it was discovered that access was also gained to an email account of a MJHS Home Care employee.

Attribution 1 Publication: hhs.gov / hipaajournal.com / NY AG's off Author:
Article Title: Elderplan, Inc.
Article URL: http://www.hipaajournal.com/mjhs-phishing-attack-result-exposure-28000-individuals-phi-8938/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-14	MJHS Home Care	NY	8/11/2017	Electronic	Medical/Healthcare	Yes - Published #	2,808

In the case of the phishing attack on MJHS, the motive of the malicious actor is unknown. The compromised email accounts were secured before the accounts could be used to send any emails, although it is possible that the protected health information of patients/plan members may have been viewed. (Number exposure per NY AG's office)

Attribution 1 Publication: hhs.gov / hipaajournal.com / NY AG's off Author:
Article Title: MJHS Phishing Attack Result in the Exposure of 28,000 Individuals' PHI
Article URL: http://www.hipaajournal.com/mjhs-phishing-attack-result-exposure-28000-individuals-phi-8938/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-13	Mercy Family Medicine	CO	8/17/2017	Electronic	Medical/Healthcare	Yes - Published #	2,069

On June 21, Centura Health found a hard drive containing historical patient information had gone missing from Durango Family Medicine. The hard drive files specific to visits at Mercy Family Medicine are limited, but may contain personal information such as patient demographics and/or clinical information, including diagnosis, progress notes, medications, vital signs and consultation notes.

Attribution 1 Publication: Becker's Health IT & CIO Review / hhs.g Author:
Article Title: Centura Health notifies Mercy Family Medicine patients about potential data breach
Article URL: http://www.beckershospitalreview.com/healthcare-information-technology/centura-health-notifies-mercy-family-medici

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-12	South Washington County Schools	MN	8/17/2017	Electronic	Educational	Yes - Unknown #	Unknown

Leaders of the South Washington County Schools apologized Thursday for a massive, accidental release of private student information sent out in an email attachment Wednesday from the district's transportation department. The attachment contains names, grades, identification numbers, email addresses, mailing addresses, phone numbers, bus routes, pick up and drop off times, pick up and drop off locations, and schools of attendance for some 9,000 students.

Attribution 1 Publication: databreaches.net / mprnews.org Author:
Article Title: Error exposes private info on thousands of South Wash. Co. students
Article URL: https://www.mprnews.org/story/2017/08/17/south-wash-co-students-private-data-exposed-error

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-11	Election Systems & Software	IL	8/17/2017	Electronic	Business	Yes - Published #	1,800,000

A leading US supplier of voting machines confirmed on Thursday that it exposed the personal information of more than 1.8 million Illinois residents. tate authorities and the Federal Bureau of Investigation were alerted this week to a major data leak exposing the names, addresses, dates of birth, partial Social Security numbers, and party affiliations of over a million Chicago residents. Some driver's license and state ID numbers were also exposed.

Attribution 1 Publication: databreaches.net / gizmodo.com Author:
Article Title: US Voting Machine Supplier Leaks 1.8 Million Chicago Voter Records
Article URL: http://gizmodo.com/us-voting-machine-supplier-leaks-1-8-million-chicago-vo-1797947510

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-10	National DCP, LLC Health Plan	GA	8/8/2017	Electronic	Medical/Healthcare	Yes - Published #	1,190

An email account was inappropriately accessed as a result of an email phishing scam in March 2017. We investigated the matter and found at that time there was no indication that sensitive data was acquired.That investigation is still ongoing, but on June 26, 2017, we were alerted that personal information was contained in the email account. Your data that could have been accessed includes your name, address, social security number, and date of birth.

Attribution 1 Publication: hhs.gov / NH AG's office / MD AG's offic Author:
Article Title: National DCP, LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/National%20DCP%20LLC%20SBN%20to%20Consumer

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-09	Juliska	CT	8/11/2017	Electronic	Business	Yes - Published #	4,949

Since learning of the incident and promptly removing the malicious code/ we initiated a full investigation with a team of digital forensic experts, which was concluded on July 18, 2017. During this time period, the information associated with website orders including name/address, email, phone number, and payment card information (including card number, expiration date and security code), may have been compromised. (Exosure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-08	St. Mark's Surgical Center	FL	8/14/2017	Electronic	Medical/Healthcare	Yes - Published #	33,877

On May 8, 20l7, following a forensic investigation by a third-party firm, St. Mark's Surgical Center, LLC (the "Center") discovered that, between April13 and April 17; 2017, it was the target of a ransomware attack that affected certain electronic files on the Center's server. The Center's server contains certain data elements of personal information for the Center's patients, including you, such as names, dates of birth, health information, treatment information, and/or Social Security numbers.

Attribution 1 Publication: VT AG's office / hhs.gov / hipaajournmal Author:
Article Title: St. Mark's Surgical Center
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/St%20Marks%20Surgical%20Center%20LLC%20SBN%

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-07	TRUEbenefits LLC	WA	8/14/2017	Electronic	Business	Yes - Published #	17,309

A phishing email was sent from the email account of an employee of TRUEbenefits on May 19, 2017, without the employee's knowledge. We conducted a thorough review of the employee's email account and determined on June 26, 2017, that an unauthorized person had access to the employee's email account and some of the emails may have contained your name<<variable data>>

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-06	American Broadband	NE	8/8/2017	Electronic	Business	Yes - Unknown #	Unknown

We recently discovered that our company was the victim of an email spoofing attack on July 28, 2017, by an individual pretending to be our Chief Financial Officer. A request was made from what appeared to be a legitimate ABB email address for all 2016 ABB employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before we discovered that the request was fraudulent.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-05	Lake Health / TriPoint Medical Center	OH	8/18/2017	Paper Data	Medical/Healthcare	Yes - Published #	750

A log book containing the protected health information of approximately 750 obstetrics patients of TriPoint Medical Center in Concord Township, Ohio has been discovered to be missing. The log book contained only limited protected health information of patients and the loss/theft of the logbook did not result in the exposure of any highly sensitive information such as Social Security numbers, financial information, or details of health insurance.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: Lake Health Informs OB Patients of TriPoint Medical Center Breach
Article URL: http://www.hipaajournal.com/lake-health-tripoint-medical-center-breach-8931/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-04	Institute for Women's Health	TX	8/21/2017	Electronic	Medical/Healthcare	Yes - Published #	15,761

That investigation revealed the malware had been installed on June 5, although it took until July 11 for the malware to be removed from the majority of its systems and a further two days for IFWH to confirm that the malware had been completely removed from all terminal servers and workstations. The types of data recorded by the malware between June 5 and July 11 includes names, dates of birth, addresses, Social Security numbers, scheduling notes, current procedural technology and other billing codes and other information that was entered into its system between those dates.

Attribution 1 Publication: hipaajournal.com / hhs.com Author:
Article Title: http://www.hipaajournal.com/institute-for-womens-health-hacked-phi-compromised-8933/
Article URL: http://www.hipaajournal.com/institute-for-womens-health-hacked-phi-compromised-8933/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-03	Golden 1 Credit Union	CA	8/4/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On August 4, 2017, we discovered that three illegal skimmer devices had been installed on ATM machines at Golden 1 branch locations in Sacramento, El Dorado, and Placer Counties. After immediately initiating an investigation, we determined that the hidden cameras used to capture PIN numbers had also been installed on these ATMs.

Attribution 1 Publication: CA AG's office Author:
Article Title: Golden 1 Credit Union
Article URL: https://oag.ca.gov/system/files/Notice%20of%20Data%20Breach%20080917_1.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-02	Dutch, LLC / Joie.com /	CA	8/22/2017	Electronic	Business	Yes - Published #	11,578

We recently learned that we were the victims of a sophisticated cyber-attack that may affect the security of your payment information. On or around July 7, 2017 it was determined that debit or credit cards used at www.joie.com between December 25, 2016 and January 26, 2017 could be impacted by this incident.

Attribution 1 Publication: CA AG's office / NY AG's office / NH AG' Author:
Article Title: Dutch, LLC / Joie.com
Article URL: https://oag.ca.gov/system/files/Dutch%20-%20Notice%20only-%20CA%20-%20Exhibit%201_0_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170822-01	Native Shoes	US	8/16/2017	Electronic	Business	Yes - Unknown #	Unknown

Native Shoes became aware of a potential vulnerability in the security of our website in late June 2017 and immediately launched an investigation. That investigation has confirmed that malware may have infected the Native Shoes website as early as April 2015. As a result, we are informing you that it is possible that your payment information was compromised if you bought shoes from nativeshoes.com using Visa or Mastercard between April 28, 2015, and June 23, 2017.

Attribution 1 Publication: NH AG's office / CA AG's office / VT AG' Author:
Article Title: Native Shoes
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/native-canada-20170816.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-17	Krell & Associates	NY	8/15/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 2, 2017 the computer forensics investigators informed Krell that based on their analysis, files containing client information may have been compromised by an unauthorized individual. The files that may have been accessed included information used to prepare tax returns, including names, addresses, Social Security numbers, wage information, and bank account information of a small number of Krell clients.

Attribution 1 Publication: CT AG's office Author:
Article Title: Krell & Associates
Article URL: per FOIA request

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-16	Harry Winston, Inc.	NY	8/15/2017	Electronic	Business	Yes - Published #	430

Based on our investigation, it appears that, on January 30, 2017, the 2016 W-2 forms of all of the U.S. employees of Harry Winston Inc. ("Harry Winston") and several former employees of Harry Winston, including your W-2 form, were inadvertently disclosed to an unknown and unauthorized outside person through an email phishing scam. (Exposure number per NY AG's office)

Attribution 1 Publication: CT AG's office / NY AG's office Author:
Article Title: Harry Winston, Inc.
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-15	Frasca International, Inc.	IL	8/15/2017	Electronic	Business	Yes - Unknown #	Unknown

e recently discovered that our company was the victim of an email spoofing attack on January 20, 2017 by an individual pretending to be our President. A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information.

Attribution 1 Publication: CT AG's office Author:
Article Title: Frasca International, Inc.
Article URL: Per FOIA CT AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-14	Intrepid Aviation Management, LLC	CT	8/15/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 2, 2017, with tax season nearing completion, Intrepid Aviation was the targeted victim of an email spoofing attack.

Attribution 1 Publication: CT AG's office Author:
Article Title: Intrepid Aviation Management, LLC
Article URL: Per FOIA CT AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-13	Ingis & Company	NJ	7/17/2017	Electronic	Business	Yes - Published #	647

On May 30, 2017, Ingis became aware of the possibility that some clients' tax information stored within their server may have been accessed by an unknown, unauthorized third-party. The investigation determined that clients' personally identifiable information ("PII"), including names, Social Security numbers and other tax information may have been accessed or viewed by at unauthorized third-party. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: Ingis & Company
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/ingis-20170714.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-12	Delek US Holdings	TN	7/26/2017	Electronic	Business	Yes - Published #	27,123

On May 23, 2017, an unknown person broke into the vehicle of a Delek employee. The laptop contained various files that may have included your name, address, Social Security number, and/or information about compensation and benefits. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / MD A Author:
Article Title: Delek US Holdings
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/delek-20170726.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-11	**Bishop Company**	MA	8/10/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On July 28, 2017, The Bishop Co. 's investigation of a suspected email phishing incident concluded . While there is no indication that this unknown individual was able to access any other accounts or systems beyond this one email account, The Bishop Co. 's investigation determined that some of its clients' information was contained in the emails, including names, Social Security numbers, and, in some instances, driver's license numbers.

Attribution 1
Publication: NH AG's office Author:
Article Title: Bishop Company
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/bishop-company-20170809.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-10	**Doctors Community Surgical Associates / Continuum**	TX	8/10/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,396**

On June 6, 2017, Continuum notified MDeverywhere that it had discovered that information contained in files on the messaging board had potentially become accessible by internet users without a user name and password. These documents contained the following information relating to you: patient name, insurance company or payor name or abbreviation, date of service, medical provider, insurance payment status information, patient date of birth, subscriber insurance ID#, patient address, patient Social Security number, procedure code and diagnosis code.

Attribution 1
Publication: hhs.gov MD AG's office Author:
Article Title: Doctors Community Surgical Associates / Continuum Health Alliance, LLC / Mdeverywhere, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-286609.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-09	**Visiting Nurse Association of New Jersey**	NJ	8/10/2017	Paper Data	Business	Yes - Unknown #	**Unknown**

The owners of Sublimation 101 printing company in Branchburg told News 12 New Jersey Wednesday that they purchased some used office furniture for their business. They said that when they opened one of the cabinets, they found hundreds of Employment Eligibility Verification forms, or I-9s, with personal information. he forms included names, addresses and phone numbers, as well as copies of Social Security cards, driver's licenses, passports and naturalization documents.

Attribution 1
Publication: databreaches.net / newjersey.news12.co Author:
Article Title: Federal officials retrieve I-9 forms found in used office furniture
Article URL: http://newjersey.news12.com/story/36102980/documents-with-sensitive-information-found-in-used-office-furniture

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-08	**Colorado Judicial Department**	CO	8/8/2017	Electronic	Government/Military	Yes - Published #	**41,140**

Files containing 620,945 names with corresponding Social Security numbers and dates of birth were exposed on the department's internal intranet. A smaller number, 41,140, names and like data, was exposed externally, available to anyone on the internet.

Attribution 1
Publication: databreaches.net / denverpost.com Author:
Article Title: State juror pool data breach exposed Social Security numbers
Article URL: http://www.denverpost.com/2017/08/08/state-juror-pool-data-breach-exposed-social-security-numbers/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-07	**Shoe Station**	AL	8/8/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On June 12, 2017, Shoe Station learned that malicious files had been detected on our e-commerce website, www.shoestation.com. The investigation has determined certain payment card information related to you may have been accessed. This information may include the following: name, address, payment card number, card expiration date, and CVV number.

Attribution 1
Publication: MT AG's office / NH AG's office / MD AG Author:
Article Title: Shoe Station
Article URL: https://dojmt.gov/wp-content/uploads/Shoe-Station.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-06	**Wooster-Ashland Regional Council of Governments**	OH	8/9/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On or about June 28, 2017, the FBI notified WARCOG that it was the victim of a cyberattack by which an unknown third-party was able to access a computer file containing the personal information of individuals listed within police incident reports originating in the Cities of Wooster, Ashland, and Orrville over the last ten years. Based on our internal investigation of this matter, we have determined that the personal information potentially at risk of being accessed included first and last names, home addresses, dates of birth, social security numbers, and driver's license numbers .

Attribution 1 Publication: MT AG's office / VT AG's office / NH AG' Author:
Article Title: Wooster-Ashland Regional Council of Governments
Article URL: https://dojmt.gov/wp-content/uploads/Wooster-Ashland-Regional-Council-of-Governments.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-05	**Marine Corps Association and Foundation**	VA	8/11/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We recently learned that our online store, which is hosted and maintained by a vendor, may have been compromised. Such information may include your name, address, telephone number, and credit or debit card information, including the expiration date and card verification number.

Attribution 1 Publication: MT AG's office / NH AG's office / MD AG Author:
Article Title: Marine Corps Association
Article URL: https://dojmt.gov/wp-content/uploads/Marine-Corps-Association-Foundation.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-04	**WNET**	NY	8/4/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On June 10, 2017, WNET determined that an unknown individual had gained access to certain WNET employees' email accounts, and that certain protected information relating to you was accessible to the unknown individual. While we currently have no evidence that the unauthorized individual actually accessed or acquired your information, we have confirmed that your name and <<data elements affected>> were accessible to the unknown individual during this event.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-03	**Surgical Dermatology Group**	AL	8/14/2017	Electronic	Medical/Healthcare	Yes - Published #	**14,000**

Hackers have gained access to a server maintained by cloud hosting and server management provider TekLinks and have potentially accessed/copied the protected health information of patients of Surgical Dermatology Group in Birmingham, AL. The types of data stored on the compromised server includes patients' names, home and work telephone numbers, cell phone numbers, addresses, email addresses, medical record numbers, patient ID numbers, Social Security numbers, health plan numbers, details of charges and payments and physicians' names.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: Surgical Dermatology Group Informs Patients of Cloud Services Provider Breach
Article URL: http://www.hipaajournal.com/surgical-dermatology-group-informs-patients-cloud-services-provider-breach-8926/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-02	**Missouri Care Inc.**	MO	8/14/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,223**

A mailing error by a subcontractor of Missouri Care Inc., has resulted in the protected health information of 1,223 participants being impermissibly disclosed to other individuals. The error potentially resulted in the names, birth dates, MO HealthNet ID numbers and Missouri Care member ID numbers of Medicaid recipients being mailed to incorrect recipients.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Missouri Care Notifies Medicaid Recipients of Subcontractor Breach
Article URL: http://www.hipaajournal.com/missouri-care-notifies-medicaid-recipients-subcontractor-breach-8924/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170815-01	Pacific Alliance Medical Center	CA	8/10/2017	Electronic	Medical/Healthcare	Yes - Published #	266,123

On June 14,2017, PAMC became aware that certain of its networked computer systems were being affected by a cyber incident. The personal information on the servers affected by the virus may have included: name, demographic information, date of birth, Social Security number, and employment information.

Attribution 1 Publication: CA AG'soffice / hipaajournal.com / hhs.g Author:
Article Title: Pacific Alliance Medical Center
Article URL: https://oag.ca.gov/system/files/Breach%20Notification%20Forms_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170809-03	HD Vest Investment Services	TX	8/9/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 15, 2017, HD Vest learned that the investigation identified malware on computer systems within Mr. Petrarca's network with the capability to provide remote access to the computer systems. Although no evidence was found to indicate data was exfiltrated from Mr. Petrarca's network, the malware had the ability to provide access to computer systems containing, or providing access to, personal information of some of Mr. Petrarca's clients, which may have included names, addresses, and Social Security numbers.

Attribution 1 Publication: CT AG's office Author:
Article Title: HD Vest Investment Services
Article URL: per FOIA request

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170809-02	George Mason University	VA	8/9/2017	Electronic	Educational	Yes - Unknown #	Unknown

On March 15, 2017, George Mason University learned that certain documents provided to the law school's Mason Veterans and Servicemembers Legal Clinic (the "M-VETS Clinic"), submitted through the M-VETS Clinic application website, inadvertently became accessible via the Internet. The information contained in the documents may have included clients' names, addresses, dates of birth, social security numbers and/or driver's license numbers.

Attribution 1 Publication: CT AG's office Author:
Article Title: George Mason University
Article URL: per FOIA request

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170809-01	GlaxoSmithKline LLC	PA	8/9/2017	Electronic	Business	Yes - Published #	4,000

On March 14, 2017, approximately 4,000 GSK employees received a phishing e-mail purportedly sent by the Company's CEO containing an attachment that, when opened, routed to a website requesting
the recipient's GSK email address and password. On March 21st GSK
became aware that a small number of employees had entered their email address and password on the website, which then allowed an unauthorized person(s) to access GSK's HR system that hosts payroll
bank routing, direct deposit information.

Attribution 1 Publication: CT AG's office Author:
Article Title: GlaxoSmithKline LLC
Article URL: per FOIA request

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-16	Sport and Spine Rehab	MD	8/5/2017	Electronic	Medical/Healthcare	Yes - Published #	31,120

On June 3rd 2017, Sport and Spine Rehab was the victim of a ransomware attack that encrypted the data stored on it's servers. SSR did determine that some files containing patient information were auto-encrypted/locked by the ransomware virus that infiltrated SSR's old system. The compromised information could include patient names, addresses, dates of birth, Social Security numbers, and medical information.

Attribution 1 Publication: benzinga.com / hhs.gov Author:
Article Title: Sport and Spine Rehab: Attention Patients Seen Prior to May 1st, 2016 - Data Breach Possibly Affects Your Account
Article URL: https://www.benzinga.com/pressreleases/17/08/r9884651/sport-and-spine-rehab-attention-patients-seen-prior-to-may-1

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-15	Southern New Hampshire University (July 2017)	NH	7/27/2017	Electronic	Educational	Yes - Unknown #	Unknown

On June 1, 2017, an unknown third-party sent a phishing e-mail message from a hacked university email address to select members of the Southern New Hampshire University ("SNHU") community. The software they accessbd using these credentials contained a section that included social security numbers and, if entered by the user, other government IDs, such as driver's license numbers.

Attribution 1 Publication: NH AG's office Author:
Article Title: Southern New Hampshire University (June 2017)
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/southern-new-hampshire-university-20170727.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-14	Southern New Hampshire University (April 2017)	NH	8/8/2017	Electronic	Educational	Yes - Unknown #	Unknown

In accordance with N.H. Rev. Stat. § 359-C:20, please accept this letter as notification of a data breach that occurred between January 6 and February 15, 2017. The software system that was accessed included the ability to view the individual employee's Social Security number, though the University was unable to confirm during the course of its investigation whether the particular page containing this information was accessed during the intrusion.

Attribution 1 Publication: NH AG's office Author:
Article Title: Southern New Hampshire University
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/southern-new-hampshire-university-20170403.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-13	Starwood Property Trust / Starwood Mortgage Capital	CT	7/7/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On our around June 19, 2017, we determined that your information may have been accessible to an unauthorized individual. We conducted a thorough review of the employee's email account and determined that it may have contained some personal ipformation, including your name, address, date of birth, bank account number, and Social Security number.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Starwood Property Trust / Starwood Mortgage Capital
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/starwood-property-20170707.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-12	Directron	TX	7/28/2017	Electronic	Business	Yes - Published #	657

On or about February 12, 2017 - April 4, 2017, transactions that our New Hampshire customers initiated on the Directron website may have been compromised and information regarding such transactions may
have been transmitted to an unauthorized third party. The information that may have been accessed included names, credit card information, CW codes, billing and shipping addresses, email addresses, and your Directron website user name and password.

Attribution 1 Publication: NH AG's office / ME AG's office / NY AG Author:
Article Title: Directron
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/directron-20170728.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-11	Citizens Financial Group (7/6)	RI	7/7/2017	Electronic	Banking/Credit/Financial	Yes - Published #	152

Our investigation into the incident determined that ATM skimming took place at a Citizen's Bank ATM located in Glastonbury, Connecticut. The skimming events took place on various dates in June 2017 and were discovered by Citizens on June 23, 2017. Customer name, debit card number, and PIN were compromised as a result ofthis incident. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Citizens Financial Group
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-20170707.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-10	**Citizens Financial Group (7/3/17)**	RI	7/3/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**4,837**

We are writing to inform you that due to a security incident at an«Line_Number» 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. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Citizens Financial Group, Inc.
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-20170703.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-09	**Citizens Financial Group (6/7/2017)**	RI	8/8/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

Our investigation into the incident determined that ATM skimming took place at a Citizen's Bank ATM located in Boston, Massachusetts. The skimming events took place on various dates in April 2017 and were discovered by Citizens on May 25, 2017. Customer name, debit card number, and PIN were compromised as a result of this incident.

Attribution 1 Publication: NH AG's office Author:
Article Title: Citizens Financial Group (6/7/2017)
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-group-20170607.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-08	**Citizens Financial Group (6/6/2017)**	RI	8/8/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

Our investigation into the incident determined that a former colleague inappropriately accessed customer information on various dates in January 2017. The personal information compromised included the customer's name, address, Social Security number, and account number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Citizens Financial Group
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-group-20170606.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-07	**Citizens Financial Group (8/2/17)**	RI	8/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**313**

The skimming events took place on various dates in June 2017 and were discovered by Citizens on July 9, 2017. Customer name, debit card number, and PIN were compromised as a result of this incident. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Citizens Financial Group
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-20170801.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-06	**BST & Co. CPAs, LLP / CCH**	NY	7/28/2017	Electronic	Business	Yes - Unknown #	**Unknown**

BST recently became aware of suspicious activity relating to certain client's personal documents stored in the online tax portal operated by CCH. This information may include the following: name, date of birth, address, driver's license number, Social Security number, financial account information, an /or medical information, if contained in the documents stored on the portal.

Attribution 1 Publication: NH AG's office Author:
Article Title: BST & Co. CPAs, LLP
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/bst-20170728.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-05	State Industrial Products / Neutron Industries	AZ	8/4/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 26, 2017, the vendor that we worked with to develop and maintain our Neutron Industries ecommerce platform, neutronindustries.com, notified us that the company who hosts neutronindustries.com identified suspicious code and subsequently disabled the site. The infonnation that may have been accessed includes your name, shipping and billing addresses, payment card number, expiration date, and card security code (CVV). In addition, if you logged in or registered through the user authentication page, the code may have accessed the username and password you use for your account.

Attribution 1 Publication: MT AG's office / MD AG's office / ME A Author:
Article Title: State Industrial Products / Neutron Industries
Article URL: https://dojmt.gov/wp-content/uploads/State-Industrial-Products.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-04	Metropolitan Life Insurance Co.	NY	7/19/2017	Electronic	Business	Yes - Published #	4,220

On July 7, 2017, an old dental claim of yours was erroneously sent to a dentist who was not your own dental provider, and that dentist was then able to view your dental information. The information viewable by the dentist included personal information such as your name, address, Social Security number and dental claims information.

Attribution 1 Publication: hhs.gov / NY AG's office Author:
Article Title: Metropolitan Life Insurance Co.
Article URL: Per FOIA request to NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-03	Christine D. Collins, APC / Ann Hofstadter, MD, Inc.	CA	7/27/2017	Electronic	Medical/Healthcare	Yes - Published #	1,500

Christine D. Collins, APC & Ann Hofstadter, MD Inc. CA Healthcare Provider 1500 07/27/2017 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Christine D. Collins, APC / Ann Hofstadter, MD, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=7104FB45E071534DC28AB4E59AAB48E0

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-02	Daniel Drake Center for Post-Acute Care / Cincinnati's UC	OH	8/4/2017	Electronic	Medical/Healthcare	Yes - Published #	4,271

Cincinnati's UC Health has discovered a former employee of its Daniel Drake Center for Post-Acute Care had been accessing the medical records of its patients without authorization for almost two years. The types of information accessed by the individual included patients' names, medical record numbers, birth dates, lab test results, diagnoses, treatment information and other clinical data.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 4,271 UC Health Patients Notified of Insider Data Breach
Article URL: http://www.hipaajournal.com/4271-uc-health-patients-notified-of-insider-data-breach-8913/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170808-01	City of Hope	CA	8/3/2017	Electronic	Medical/Healthcare	Yes - Published #	3,400

Despite all of the measures that we implement to protect our patients' information, we recently learned that City of Hope was the target of a phishing email. he information in the email accounts may have included your name, medical record number, date of birth, address, email address, telephone number and clinical information such as diagnosis, diagnostic test results, medication information or dates of service.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
Article Title: City of Hope
Article URL: https://oag.ca.gov/system/files/Patient%20Notification%20Letter_2.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170802-08	Forest Hill Health & Rehab Center	IL	7/31/2017	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

Though local, state and federal authorities know that medical records have been stolen from the old nursing home, no one can agree on who is responsible for securing the building. "With respect to the medical records and personnel records currently in the building — the overwhelming majority of the records appear to be centralized in three offices/closets. The records are in file boxes, and are stacked in these rooms from floor to ceiling, front to back. A rough estimate would be 400+ file boxes of records."

Attribution 1 Publication: databreaches.net / qctimes.com Author:
Article Title: Ickes: No one taking responsibility for exposed medical records at Forest Hill
Article URL: http://qctimes.com/news/local/barb-ickes/ickes-no-one-taking-responsibility-for-exposed-medical-records-at/article_86

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170802-07	Northwest Rheumatology	AZ	8/1/2017	Electronic	Medical/Healthcare	Yes - Published #	7,468

On April 10, 2017, Northwest Rheumatology ("NW Rheumatology") experienced a ransomware incident which left a limited portion of its computer system encrypted and inaccessible.

Attribution 1 Publication: databreaches.net / hipaajournal.com / N Author:
Article Title: Northwest Rheumatology of Tucson Notifies Patients of Potential Data Security Incident
Article URL: https://www.databreaches.net/northwest-rheumatology-of-tucson-notifies-patients-of-potential-data-security-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170802-06	Daniel Drake Center for Post-Acute Care	OH	8/2/2017	Electronic	Medical/Healthcare	Yes - Published #	4,721

UC Health's privacy office was notified June 2 that a Drake hospital employee had accessed medical records without authorization between that day and July 29, 2015. Information that might have been viewed included the patients' names, addresses, dates of birth, medical record numbers, diagnosis/condition, lab results, treatment and medication information, according to UC Health. The patients' full Social Security numbers were not included with the information.

Attribution 1 Publication: databreaches.net / bizjournals.com / hhs Author:
Article Title: UC Health hospital notifies patients of medical records being compromised
Article URL: https://www.bizjournals.com/cincinnati/news/2017/08/02/uc-health-hospitalnotifies-patients-of-medical.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170802-05	Capital One 360	MN	7/31/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

A former employee may have accessed your information between January 27, 2017 through April 20, 2017 when they shouldn't have. While we do not see any suspicious account transactions related to this, please keep an eye out for unauthorized transactions (including outside of Capital One®) because the person saw your account information, such as your name, address, account number, telephone number, transaction history, date of birth and Social Security Number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170802-04	Kentucky Wesleyan College	KY	7/26/2017	Electronic	Educational	Yes - Published #	6,100

On April 21, 2017, we discovered that Kentucky Wesleyan College had become the target of a phishing email campaign and that several employees had clicked on the phishing email and entered their credentials. While we currently have no evidence that the unauthorized individual or individuals actually accessed or acquired your information, we have confirmed that your name and <<data elements affected>> were accessible to the unknown actor during this event. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's offce / MD AG's office / NY AG' Author:
Article Title: Kentucky Wesleyan College
Article URL: https://dojmt.gov/wp-content/uploads/Kentucky-Wesleyan-College.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170802-03	**Kevin J Palmer**	CA	7/25/2017	Electronic	Business	Yes - Published #	**1,438**

We discovered a cyberattack on our system on June 6th, 2017. Documents could include your: Documents could include your: full name, telephone number(s), address, Social Security Number, all employment W-2 information if applicable, 1099 information if applicable (which may include account number if provided), direct deposit bank account information (including account number and routing number if provided), email addresses (if provided), and supporting records. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / MD AG's office / NY A Author:
Article Title: Kevin J Palmer
Article URL: https://dojmt.gov/wp-content/uploads/Kelvin-J-Palmer-Co.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170802-02	**Cole Sport**	UT	7/28/2017	Electronic	Business	Yes - Unknown #	**Unknown**

This incident relates to the unauthorized acquisition, by hackers, of certain information entered by customers on the Cole Sport online store checkout page. The information compromised varies by individual, but may include a customer's name, shipping and billing address, email address, payment card type, payment card number, expiration date, and verification number, and potentially, the user's colesport.com account password.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170802-01	**UCLA Summer Sessions & International Education Office**	CA	7/31/2017	Electronic	Educational	Yes - Published #	**32,000**

On May 18, 2017,we determined that an attacker gained unauthorized access to a Summer Sessions & International Education Office server that contained personal information provided by students, such as their names, addresses, dates of birth, social security numbers, health insurance subscriber IDs, and some medical information self-reported by students (e.g., allergies, medical conditions, medications, etc.).

Attribution 1 Publication: CA AG's office / databreaches.net / daily Author:
Article Title: UCLA Summer Sessions & International Education Office
Article URL: https://oag.ca.gov/system/files/UCLA-SS%26IEO-notification-letter_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170801-04	**Kennebunk Center for Dentistry**	ME	7/3/2017	Paper Data	Medical/Healthcare	Yes - Published #	**1,900**

Kennebunk Center for Dentistry ME Healthcare Provider 1900 07/03/2017 Unauthorized Access/Disclosure Electronic Medical Record, Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Kennebunk Center for Dentistry
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=0667A26D179973E81E7DE463405B983E

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170801-03	**Braun Internal Medicine, P.C.**	GA	7/14/2017	Electronic	Medical/Healthcare	Yes - Published #	**680**

Braun Internal Medicine, P.C. GA Healthcare Provider 680 07/14/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Braun Internal Medicine, P.C.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=0667A26D179973E81E7DE463405B983E

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170801-02	**Sage Dental Management**	FL	7/19/2017	Electronic	Medical/Healthcare	Yes - Published #	**5,000**

SAGE DENTAL MANAGEMENT, LLC FL Business Associate 5000 07/19/2017 Theft Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Sage Dental Management
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=0667A26D179973E81E7DE463405B983E

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170801-01	**Kaleida Health**	NY	7/21/2017	Electronic	Medical/Healthcare	Yes - Published #	**2,789**

On May 24, 2017, we learned that an unauthorized third party potentially accessed a Kaleida Health employee's email account. The investigation determined that an unauthorized third party may have gained access to a small number of Kaleida Health email accounts, which may have included patients' names, medical record numbers, dates of birth, diagnoses, treatment information, or other clinical information.

Attribution 1 Publication: hhs.gov / databreaches.net/ Kaleida He Author:
Article Title: NY: Kaleida Health notifies 2,789 patients about phishing incident
Article URL: https://www.databreaches.net/ny-kaleida-health-notifies-2789-patients-about-phishing-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170731-02	**Plastic Surgery Associates of South Dakota**	SD	7/28/2017	Electronic	Medical/Healthcare	Yes - Published #	**10,229**

Plastic Surgery Associates of South Dakota discovered ransomware had been installed on some of its systems on February 12, 2017. The system that the ransomware was installed on contained names, Social Security numbers, driver's license numbers, state ID numbers, credit and debit card information, lab test results, medical diagnoses, birth dates, health insurance information and details of medical conditions.

Attribution 1 Publication: hiapaajournal.com / hhs.gov Author:
Article Title: 10,000 Plastic Surgery Patients Informed of Ransomware-Related PHI Breach
Article URL: http://www.hipaajournal.com/10000-plastic-surgery-patients-informed-of-ransomware-related-phi-breach-8904/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170731-01	**Steel Technology, LLC dba Hydro Flask**	OR	7/28/2017	Electronic	Business	Yes - Published #	**336**

On or about May 2, 2017, Hydro Flask learned that the security of personal information Hydro Flask received about you during your visit to our e-commerce website (http://www.hydroflask.com/) may have been compromised. Although Hydro Flask is still investigating the scope of the disruption, Hydro Flask believes that an intruder may have had unauthorized access to customer order pages on our website that may have contained your name, billing and shipping address, email address, and credit card information. (Exposure number per NY AG's office / notification from Discover)

Attribution 1 Publication: CA AG's office / MD AG's office / NY AG Author:
Article Title: Steel Technology, LLC dba Hydro Flask
Article URL: https://oag.ca.gov/system/files/HydroFlask%20-%20Sample%20Customer%20Notice_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170728-08	**Hamilton Zanze Real Estate Investments**	CA	7/27/2017	Electronic	Business	Yes - Published #	**1,140**

On June 29, 2017, an HZ employee became the victim of a crime when his locked vehicle, together with the car next to it, was broken into while parked in a Whole Foods parking garage. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / MD AG Author:
Article Title: HamiltonZanze Real Estate Investments
Article URL: https://oag.ca.gov/system/files/HZ%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170728-07	Hilderbrand & Clark	CA	7/28/2017	Electronic	Business	Yes - Published #	2,230

On Monday, July 10, 2017, the specialized forensic IT firm determined that there was unauthorized access to our system. If Hilderbrand & Clark prepared tax returns for you, the information may have included all information provided to the taxing authorities including your: full name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, all 1099 information (including account number if provided to us), driver's license information (if provided to us), and direct deposit bank account information (including account
number and routing information if provided to us). (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MD AG's office / NY AG Author:
Article Title: Hilderbrand & Clark
Article URL: https://oag.ca.gov/system/files/Hilderbrand%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170728-06	Virgin America Systems	CA	7/28/2017	Electronic	Business	Yes - Published #	3,230

On March 13, 2017, during security monitoring activities, our data security team identified potential unauthorized access to certain Virgin America computer systems. The threat actors managed to compromise login information and password that is used to access the Virgin America's corporate network of 3120 employees and even more personal information including addresses, social security numbers, details of government-issued IDs (such as driving licenses), and health-related information for an additional 110 employees.

Attribution 1 Publication: CA AG's office / scmagazine.com Author:
Article Title: Virgin America Systems
Article URL: https://oag.ca.gov/system/files/Notification%20Letter%20-%20California_0.pdf?

Attribution 2 Publication: scmagazine.com / MD AG's office Author:
Article Title: Virgin America data breach hits employees and contractors
Article URL: https://www.scmagazine.com/virgin-america-data-breach-hits-employees-and-contractors/article/678201/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170728-05	Neiman Marcus Mobile App	TX	7/28/2017	Electronic	Business	Yes - Unknown #	Unknown

Neiman Marcus has detected that, in January 2016, unauthorized individuals began attempting to try various login and password combinations using automated attacks on our mobile app environment. We suspect this activity was due to large breaches at other companies (not associated with Neiman Marcus), in which user login names and passwords were stolen.

Attribution 1 Publication: CA AG's office Author:
Article Title: Neiman Marcus Mobile App
Article URL: https://oag.ca.gov/system/files/Consumer%20Notification%20Letter%20_7-26-2017_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170728-04	Hathaway-Sycamores Child and Family Services	CA	7/28/2017	Electronic	Business	Yes - Unknown #	Unknown

We are writing to notify you of a potential data security incident that may have resulted in the disclosure of personal information regarding our employees, including names, addresses, social security numbers, and 2016 W-2 forms.

Attribution 1 Publication: CA AG's office Author:
Article Title: Hathaway-Sycamores Child and Family Services
Article URL: https://oag.ca.gov/system/files/Sample%20Notification%20Letter_2.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170728-03	Women's Health Care Group of PA, LLC	PA	7/15/2017	Electronic	Medical/Healthcare	Yes - Published #	300,000

In May, a virus was installed on a server/workstation preventing the hospital from accessing patient data. The types of data exposed – and potentially stolen – include names, addresses, dates of birth, lab test orders, lab test results, blood types, race, gender, pregnancy status, medical record numbers, employer information, insurance details, medical diagnoses, physicians' names and Social Security numbers.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Women's Health Care Group of PA, 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
ITRC20170728-02	**Braun Dermatology & Skin Cancer Center**	DC	7/28/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,200**

Braun Dermatology & Skin Cancer Center DC Healthcare Provider 1200 07/28/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Braun Dermatology & Skin Cancer Center
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170728-01	**Anthem, Inc. / Empire Health Choice HMO, Inc. /**	IN	7/24/2017	Electronic	Medical/Healthcare	Yes - Published #	**18,580**

Anthem's latest breach headache underscores the security risks posed by business associates - and their employees. In a statement, Anthem says the incident - which potentially affects Medicare members of all Anthem companies and subsidiaries - involved a former employee of Launchpoint Ventures, an Indiana-based vendor that provides Anthem with insurance coordination services. Potentially compromised information includes Medicare ID numbers - which includes a Social Security number, health plan ID numbers, Medicare contract numbers and dates of enrollment.

Attribution 1 Publication: hhs.gov / media notice / healthcareinfos Author:
Article Title: Anthem's Latest Headache: Business Associate Breach
Article URL: http://www.healthcareinfosecurity.com/anthems-latest-headache-business-associate-breach-a-10155?rf=2017-07-28_E

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170727-01	**Galt House / Al J. Schneider Company**	KY	7/26/2017	Electronic	Business	Yes - Published #	**1,411**

Malware was installed on the credit card processing system which allowed access to guests' names, credit card numbers, expiration dates and verification codes. (Al J. Schneider Company) (Exposure number per NY AG's office / notification from Discover)

Attribution 1 Publication: wave3.com / NH AG's office / MD AG's o Author:
Article Title: Galt House warns of data breach
Article URL: http://www.wave3.com/story/35981348/galt-house-warns-of-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170725-08	**Dermatology Center of Raleigh, PA**	NC	7/5/2017	Electronic	Medical/Healthcare	Yes - Published #	**3,000**

The Dermatology Center of Raleigh PA NC Healthcare Provider 3000 07/05/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Dermatology Center of Raleigh, PA
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170725-07	**Performance Physical Therapy and Wellness**	CT	7/21/2017	Electronic	Medical/Healthcare	Yes - Published #	**571**

Performance Physical Therapy and Wellness CT Healthcare Provider 571 07/21/2017 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Performance Physical Therapy and Wellness
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170725-06	**University of Mississippi Medical Center**	MS	7/7/2017	Electronic	Medical/Healthcare	Yes - Published #	**7,492**

University of Mississippi Medical Center MS Healthcare Provider 7492 07/07/2017 Hacking/IT Incident Electronic Medical Record, Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: University of Mississippi 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
ITRC20170725-05	**Unconditional Love, Inc.**	FL	7/7/2017	Paper Data	Medical/Healthcare	Yes - Published #	**643**

Unconditional Love, Incorporated FL Healthcare Provider 643 07/07/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Unconditional Love, 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
ITRC20170725-04	**Office of Paul C. Gering**	OR	7/25/2017	Electronic	Medical/Healthcare	Yes - Published #	**2,000**

Paul C. Gering, Jr., M.D. OR Healthcare Provider 2000 06/29/2017 Theft Desktop Computer

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Paul C. Gering
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=7DCC74EBBA09885832B0338A8F843049

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170725-03	**Brigham Young University**	UT	7/12/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

During a routine cybersecurity review of its information technology ("IT') systems on June 19, 2017, Brigham Young University ("BYU") observed unusual activity in connection with a web server that supports certain BYU expense reporting and financial applications. We believe that personal information relating to you, including your [data elements], may have been included in the documents that may have been accessed and acquired by the unauthorized actors.

Attribution 1 Publication: NH AG's office / ME AG's office / NY AG Author:
Article Title: Brigham Young University
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/brigham-young-20170712.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170725-02	**Atlantis Paradise Island Resort / Island Hotel**	FL	7/24/2017	Electronic	Business	Yes - Unknown #	**Unknown**

The owners of Atlantis, Paradise Island resort in the Bahamas – frequented by American tourists – has reported a data breach involving the payment network serving the resort's food and beverage and retail businesses. The company says credit and debit cards used to make purchases at those locations within the resort between November 1, 2016 and April 3, 2017 may have been compromised. Cards used to pay for room charges were not affected.

Attribution 1 Publication: Consumeraffairs.com / NY AG's office Author:
Article Title: Data breach reported at Atlantis, Paradise Island resort
Article URL: https://www.consumeraffairs.com/news/data-breach-reported-at-atlantis-paradise-island-resort-072417.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170725-01	de Arrigoitia & Co., PA	FL	7/19/2017	Electronic	Business	Yes - Published #	1,139

On June 7, 2017, DAC learned that an unauthorized individual may have gained access to our systems. The forensic investigation determined that an unauthorized individual accessed our system and may have gained access to the tax preparation software, which stores your tax information, including your name, address, Social Security number, wage information and bank account information, if you provided it to us. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: de Arrigoitia & Co., PA
Article URL: https://dojmt.gov/wp-content/uploads/de-Arrigoitia-Co.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-11	University of Vermont Medical Center	VT	7/21/2017	Electronic	Medical/Healthcare	Yes - Published #	2,300

On May 24, 2017, we learned an unauthorized third party gained access to an employee's email account on May 22, 2017. Our investigation determined an email in the account contained patient information, which may have included patients' names, addresses, dates of birth, medical record numbers, and clinical information, such as diagnoses, treatment, physicians' names and medications.

Attribution 1 Publication: vtdigger.org / hipaajournal.com / VT AG' Author:
Article Title: Email scam exposes patient records at UVM Medical Center
Article URL: https://vtdigger.org/2017/07/25/email-scam-exposes-patient-records-uvm-medical-center/

Attribution 2 Publication: Databreaches.net / Vtdigger.org Author:
Article Title: University of Vermont Medical Center notifies 2,300 patients of phishing incident
Article URL: https://www.databreaches.net/university-of-vermont-medical-center-notifies-2300-patients-of-phishing-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-10	Blue Cross Blue Shield of Tennessee	TN	7/21/2017	Electronic	Medical/Healthcare	Yes - Published #	21,000

Because of the glitch, 657 employers who have accounts with BCBST received information meant for other companies through the erroneous mailing of a report called the June 2017 Future Termination of Dependent Coverage. In the report was member names, dates of birth, plan type and coverage dates, and member identification numbers for 2,100 people.

Attribution 1 Publication: databreaches.net / Tennessean.com Author:
Article Title: BCBST glitch sends erroneous reports to 657 employers
Article URL: http://www.tennessean.com/story/money/industries/health-care/2017/07/21/bcbst-glitch-sends-erroneous-reports-657-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-09	SportsMemorabilia.com.	FL	7/18/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 29, 2017 we received a report regarding payment card activity that caused us to investigate and subsequently identify unauthorized computer code that was added to the code that operates the checkout page of www.sportsmemorabilia.com. The information on the checkout page that the code could have potentially accessed includes name, address, phone number, email address, payment card number, expiration date, and card security code (CVV).

Attribution 1 Publication: MT AG's office / MD AG's office / NY AG Author:
Article Title: SportsMem, Inc. /SportsMemorabilia.com.
Article URL: https://dojmt.gov/wp-content/uploads/SportsMem.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-08	Whitinger & Company LLC	IN	7/18/2017	Electronic	Business	Yes - Unknown #	Unknown

On April 12, 2017, we determined that there was unauthorized access to client data beyond the file encryption. The investigation has determined certain personal information related to you may have been accessed. This information may include the following categories of information: name, date of birth, address, driver's license number, Social Security number, financial account information, and/or medical information, if contained in your individual tax file.

Attribution 1 Publication: VT AG's office / MT AG's office / MD AG' Author:
Article Title: Whitinger & Company LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Whitinger%20&%20Company,%20LLC%20SBN%20to%

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-07	Keller Williams Realty, Inc.	TX	7/19/2017	Electronic	Business	Yes - Published #	398,142

We recently learned that an unauthorized third party was able to gain access to portions of the Keller Williams network and, while on the network, may have been able to access certain associate files stored in our systems. We believe that certain associate information, including first and last name, addresses, Social Security number, and in some cases, Keller Williams usernames and passwords, were contained in these files and could be affected as a result of this incident.

Attribution 1 Publication: VT AG's office / OR AG's office / MT AG' Author:
Article Title: Keller Williams Realty, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Keller%20Williams%20Realty,%20Inc.%20SBN%20to%

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-06	Chizner & Company LLC	NY	7/14/2017	Electronic	Business	Yes - Published #	1,443

On or about June 30, 2017, Chizner became aware of suspicious tax-related activity and potential unauthorized access to our tax account management and filing system. If you are a Chizner client, or a spouse of a Chizner client, your name, Social Security number, address, tax refund information, financial account information, and other information associated with your tax return were involved. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NY AG's office Author:
Article Title: Chizner & Company LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Chizner%20&%20Company%20CPA's%20LLC%20SBN

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-05	Bedrock Manufacturing Company, LLC	TX	7/14/2017	Electronic	Business	Yes - Published #	965

Unfortunately, we recently discovered that an individual or individuals hacked into the company email system and accessed a small number of users' mailboxes. The incident took place between March and June of 2017, and, during this incident, the hacker had access to certain of your personal information including your name, address, and Social Security number.

Attribution 1 Publication: VT AG's office / MT AG's office / NH AG' Author:
Article Title: Bedrock Manufacturing Company, LLC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Bedrock%20Manufacturing%20Company,%20LLC%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-04	Wells Fargo	CA	7/24/2017	Electronic	Banking/Credit/Financial	Yes - Published #	50,000

Earlier this month a lawyer for the bank allegedly sent confidential information primarily on wealthy Wells Fargo Advisors clients to a lawyer for Gary Sinderbrand, a former Wells Fargo Advisors rep involved in a defamation suit against an employee of the bank, the New York Times reports. The data came in response to Sinderbrand's lawyer's subpoena of the bank for documents and emails, according to the paper. Instead, Angela Turiano, a lawyer with Bressler, Amery & Ross, which had been hired by Wells Fargo for the suit, sent Sinderbrand 1.4 gigabytes of data that included clients' names, Social Security numbers, value of assets under management, portfolio performance and fees paid to Wells Fargo, the Times writes.

Attribution 1 Publication: financialadvisoriq.com Author:
Article Title: Wells Fargo Red-Faced Over Massive Data Breach
Article URL: http://financialadvisoriq.com/c/1690373/195503

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-03	**Tewksbury Hospitals / Department of Public Health**	MA	7/24/2017	Electronic	Government/Military	Yes - Published #	**1,176**

In response to the complaint, the hospital conducted a full review which revealed the former patient's medical records had been accessed by an employee without any legitimate reason for doing so. The types of information that were potentially accessed includes names, phone numbers, addresses, gender, dates of birth, medical diagnoses, details of medical treatment provided at the hospital and in some cases, Social Security numbers.

Attribution 1 Publication: hipaajournal.com / hhs/gov Author:
Article Title: Hospital Employee Discovered to Have Accessed Medical Records Without Authorization for 14 Years
Article URL: http://www.hipaajournal.com/hospital-employee-discovered-accessed-medical-records-without-authorization-14-years

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-02	**Vision Care Specialists**	CO	7/24/2017	Paper Data	Medical/Healthcare	Yes - Published #	**70**

However, a burglary at Vision Care Specialists' administrative offices in Denver, CO saw paperwork containing the PHI of patients taken by thieves. he documents contained a range of sensitive information including names, dates of birth, Social Security numbers, medical information, health conditions/diagnoses, financial information and health insurance details.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Protected Health Information Stolen in Vision Care Specialists Burglary
Article URL: http://www.hipaajournal.com/protected-health-information-stolen-in-vision-care-specialists-burglary-8896/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170724-01	**Value Eyecare Network, Inc. dba 39dollarglasses.com**	NY	7/21/2017	Electronic	Medical/Healthcare	Yes - Published #	**3,807**

On June 8, 2017, we learned that an unknown individual may have accessed your credit or debit card information used to make purchases at our online store. We immediately took action and commenced an investigation to determine what information may have been accessed. We determined that the unknown individual may have accessed customer payment card information, including name, address, telephone number, and credit/debit card information. (Exposure number per NY AG's office)

Attribution 1 Publication: NY AG's office Author:
Article Title: Value Eyecare Network, Inc. dba 39dollarglasses.com
Article URL: Per FOIL NY AG's office (per notification from Discover)

Attribution 2 Publication: CA AG's office / OR AG's office / MD AG Author:
Article Title: Value Eyecare Network, Inc. dba 39dollarglasses.com
Article URL: https://oag.ca.gov/system/files/39DollarGlasses%20notice%20only_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170719-01	**Dow Jones & Company**	NY	7/17/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**2,200,000**

The UpGuard Cyber Risk Team can now report that a cloud-based file repository owned by financial publishing firm Dow Jones & Company, that had been connfigured to allow semi-public access, exposed the sensitive personal and financial details of millions of the company's customers

Attribution 1 Publication: upguard.com / scmagazine.com / WI AG Author:
Article Title: Cloud Leak: WSJ Parent Company Dow Jones Exposed Customer Data
Article URL: https://www.upguard.com/breaches/cloud-leak-dow-jones

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170718-15	**QBE North America**	WI	7/3/2017	Electronic	Business	Yes - Published #	**132**

QBE was subject to a phishing attack that targeted QBE North America employee email accounts on May 31 , 2017. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MT AG's office / MD AG Author:
Article Title: QBE North America
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/qbe-20170703.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170718-14	Open Text Corporation	US	7/6/2017	Electronic	Business	Yes - Published #	300

Open Text has learned that on Sunday, June 25, 2017, a storage device was stolen which we believe may have contained personal information for certain current and former employees as of 2014. We believe that the storage device may have contained the following types of information as of 2014: Employee's name, date of birth, address, dates of employment, education history, salary, copy of Employee's Passport Bio page, which may include information such as the Employee's citizenship, place of birth and passport number and more. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / ME A Author:
Article Title: Open Text Corporation
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/open-text-20170706.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170718-13	Nathan Sports	CA	7/18/2017	Electronic	Business	Yes - Published #	330

On April 6, 2017, Nathan discovered that your personal information may have been affected when an external actor or actors placed hidden code on the Nathan webservers (the " Incident"). The code may have targeted certain personal information of customers who made credit card purchases via the Nathan webservers between September 5, 2016 and November 11 , 2016, including those customers' first and last names, billing or mailing addresses, e-mail addresses and credit card information (card holder names, credit card account numbers, expiration months and years and card security codes). Per FOIL NY AG's office

Attribution 1 Publication: NH AG's office / ME AG's office / NY A Author:
Article Title: Nathan Sports
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/nathan-sports-20170501.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170718-12	White Coats Wellness	FL	7/10/2017	Electronic	Medical/Healthcare	Yes - Published #	10,000

White Coats Wellness FL Business Associate 10000 07/10/2017 Hacking/IT Incident Email

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170718-11	S and S Dental Group dba Kennebunk Center for	ME	7/3/2017	Electronic	Medical/Healthcare	Yes - Published #	1,900

S and S Dental Group DBA Kennebunk Center for Dentistry ME Healthcare Provider 1900 07/03/2017 Unauthorized Access/Disclosure Electronic Medical Record, Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: S and S Dental Group dba Kennebunk Center for Dentistry
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170718-10	Rosalind Franklin University of Medicine	IL	7/9/2017	Electronic	Medical/Healthcare	Yes - Published #	859

The protected health information of 859 patients of Rosalind Franklin University of Medicine and Science (RFU) has been compromised and potentially been viewed/stolen. The information was stored in two email accounts that were accessed by unauthorized individuals in May. Access to the email accounts was gained after employees responded to phishing emails.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Rosalind Franklin University of Medicine
Article URL: http://www.hipaajournal.com/rosalind-franklin-university-medicine-science-phishing-attack-sees-phi-compromised-88

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170718-09	Pharma Medica Research, Inc.	MO	7/18/2017	Electronic	Medical/Healthcare	Yes - Published #	2,718

Pharma Medica Research Inc. MO Healthcare Provider 2718 06/23/2017 Hacking/IT Incident Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Pharma Medica Research, 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
ITRC20170718-08	Ledet Family Chiropractic Center	PA	7/9/2017	Electronic	Medical/Healthcare	Yes - Published #	530

Ledet Family Chiropractic Cener PA Healthcare Provider 530 07/09/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Ledet Family Chiropractic 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
ITRC20170718-07	LC&Z General and Cosmetic Dentistry	FL	7/11/2017	Electronic	Medical/Healthcare	Yes - Published #	4,391

LC&Z General and Cosmetic Dentistry FL Healthcare Provider 4391 07/11/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: LC&Z General and Cosmetic Dentistry
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170718-05	Henry Ford Health System	MI	7/18/2017	Paper Data	Medical/Healthcare	Yes - Published #	596

Henry Ford Health System MI Healthcare Provider 596 06/26/2017 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Henry Ford 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
ITRC20170718-04	California Pacific Orthopaedics and Sports	CA	7/18/2017	Electronic	Medical/Healthcare	Yes - Published #	2,263

California Pacific Orthopaedics and Sports Medicine CA Healthcare Provider 2263 06/30/2017 Theft Laptop, Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: California Pacific Orthopaedics and Sports Medicine
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170718-03	Bay Area Pain and Wellness Center	CA	7/18/2017	Electronic	Medical/Healthcare	Yes - Published #	548

Bay Area Pain and Wellness Center CA Healthcare Provider 548 06/14/2017 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Bay Area Pain and Wellness 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
ITRC20170718-01	**Apartment Management Consultants, LLC**	UT	7/14/2017	Electronic	Business	Yes - Published #	**2,400**

Between June 29 and July 3, 2017, it is believed that outside hackers accessed AMC's payroll system through the use of malware, and attempted to change the direct deposit account information for a limited number of AMC employees. Because the hacker had access to AMC payroll information, they may have also been able to view/access other personal information of AMC employees.

Attribution 1 Publication: OR AG's office / MD AG's office / NY AG Author:
Article Title: Apartment Management Consultants, LLC
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/210238133

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170714-02	**Harvest Bible Chapel dba Walk in the Word Ministries**	IL	7/14/2017	Electronic	Business	Yes - Published #	**13,961**

On May 30, 2017, we were notified by our third-party e-commerce provider that an unknown individual may have accessed your credit card, debit card, or checking account information used to donate to WITW on our website. We determined that the unknown individual may have accessed payment information, including name, address, telephone number, credit/debit card, or checking account information depending on the form of payment you used on our website. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MD AG's office / NY Ag' Author:
Article Title: Harvest Bible Chapel dba Walk in the Word Ministries
Article URL: https://oag.ca.gov/system/files/Harvest%20Bible%20Chapel%20dba%20Walk%20in%20the%20Word%20Ministries%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170714-01	**Colorado Medicaid / DXC Technology**	CO	7/13/2017	Electronic	Medical/Healthcare	Yes - Published #	**822**

The technology company (DXC) and the Colorado Department of Health Care Policy and Financing, which manages the Medicaid program, said a security review determined that the “protected health information” of 822 people was “potentially accessible” from March 1 to May 10.

Attribution 1 Publication: denverpost.com Author:
Article Title: Colorado Medicaid system data breach potentially exposed private information of 822 people
Article URL: http://www.denverpost.com/2017/07/13/colorado-medicaid-system-data-breach-exposed-private-information-822-peopl

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-12	**Verizon**	NJ	7/13/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Verizon confirmed that a recent security incident exposed the personal identification numbers and other private information pertaining to millions of telecom customers. Each record also contained hundreds of fields of additional data, including a customer's home address, email addresses, what kind of additional Verizon services a subscriber has, the current balance of their account, and if a subscriber has a Verizon federal government account, to name a few. Each record included a customer's name, a cell phone number, and their account PIN -- which if obtained would grant anyone access to a subscriber's account, according to a Verizon call center representative, who spoke on the condition of anonymity as they were not authorized to speak to the press.

Attribution 1 Publication: washingtontimes.com Author:
Article Title: Verizon Security Breach: Data Of 6 Million Users At Risk
Article URL: http://www.washingtontimes.com/news/2017/jul/13/millions-verizon-customers-impacted-security-breac/

Attribution 2 Publication: zdnet.com / WI AG's office / MD AG's off Author:
Article Title: Millions of Verizon customer records exposed in security lapse
Article URL: http://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-11	Auburn University	AL	7/3/2017	Electronic	Educational	Yes - Unknown #	Unknown

We are contacting you regarding a data security incident recently discovered at Auburn University on June 23, 2017. As a result of this incident involving compromised Auburn University credentials, your social security number may have been exposed to others.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-10	Betty Lou's, Inc.	OR	7/13/2017	Electronic	Business	Yes - Published #	453

On May 19, 2017, Betty Lou's Inc. ("Betty Lou's") discovered that malicious code was injected directly into Betty Lou's website's source code via a non-secure FTP. The information that was exposed included first and last name, address, phone number, credit card number, and order history. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / MD AG's office / NY AG Author:
Article Title: Betty Lou's, Inc.
Article URL: https://dojmt.gov/wp-content/uploads/Betty-Lous.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-09	Community Link	WI	7/13/2017	Electronic	Medical/Healthcare	Yes - Published #	5,509

On May 3, 2017, our Information Technology Security Team discovered that an unauthorized party had gained access to one of our employee's work email accounts. We immediately locked down the email account and began an investigation which showed that the actor had access to the employee's email account from 9:49 a.m. until 1:52 p.m. on May 3, 2017. An email contained in the employee's account contained your information including your first and last name and social security number.(Exposure number per NY AG's office)

Attribution 1 Publication: hhs.gove / MT AG's office / NY AG's offi Author:
Article Title: Community Link
Article URL: https://dojmt.gov/wp-content/uploads/Community-Link.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-08	Spark Pay Online Store - multiple businesses	VA	7/10/2017	Electronic	Business	Yes - Unknown #	Unknown

We discovered malicious code on [merchant website]. The code was designed to allow fraudsters to obtain customer payment information. Based on our investigation, we believe the fraudster may have accessed your name, address, phone number, email address, payment card number, expiration date, and ON for any transactions you made on [merchant website] between [variable dates between April10, 2017 and June 7, 2017].

Attribution 1 Publication: VT AG's office / MT AG's office / CA AG' Author:
Article Title: Spark Pay Online Store - multiple businesses
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Spark%20Pay%20Online%20Store%20SBN%20to%20C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-06	Peachtree Neurological Clinic, PC	GA	7/10/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Recently, PNC's computer system was infected by a ransomware virus that encrypted our electronic medical records ("EMR") system containing our patients' medical records. We are not able to confirm which, if any, tiles or patient information were accessed by these unauthorized individuals, but it is possible that they could have accessed our EMR system and information including your name, address, telephone number, social security number, date of birth, driver's license number, treatment or procedure information, prescription information, and/or healthcare insurance information.

Attribution 1 Publication: VT AG's office / MT AG's office / hipaajo Author:
Article Title: Peachtree Neurological Clinic, PC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Peachtree%20Neurological%20Clinic%20SBN%20to%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-05	**Golf & Ski Warehouse, Inc.**	NH	7/7/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We recently learned that we were the victims of a sophisticated cyber-attack that may affect the security of your payment information. In mid-May, 2017, we determined that these files were signs of a sophisticated cyber-attack that resulted in the potential compromise of some customers' debit and credit card data used at www.golfskiwarehouse.com between March 8, 2016 and April 13, 2017.

Attribution 1 Publication: VT AG's office / MT AG's office / MD AG' Author:
Article Title: Golf & Ski Warehouse, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Golf%20&%20Ski%20Warehouse,%20Inc.%20SBN%20t

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-04	**Pacific Science Center**	WA	7/10/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Pacific Science Center was the victim of a "spear phishing" attack on June 13, 2017 and June 21, 2017 by an individual or individuals pretending to be a member of Pacific Science Center's management team. Unfortunately, copies of all 2016 employee W-2 forms were provided on both dates before the company discovered that the requests were fraudulent.

Attribution 1 Publication: WA AG's office / MT AG's office Author:
Article Title: Pacific Science Center
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Safeguarding_Consumers/Breach%20PacificScien

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-03	**Detroit Medical Center**	MI	7/13/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,529**

The Detroit Medical Center (DMC) has alerted more than 1,500 of a data breach caused by an employee who shared personal information with unauthorized individuals.

Attribution 1 Publication: scmagazine.com / hipaajournal.com Author:
Article Title: Staffing agency employee allegedly distributes patient information illegally
Article URL: https://www.scmagazine.com/staffing-agency-employee-allegedly-distributes-patient-information-illegally/article/67472

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-02	**Princeton Community Hospital**	WV	7/13/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

The Princeton Community Hospital in Mercer County will have to replace nearly 1,200 hard drives on computers that were hacked earlier this week.

Attribution 1 Publication: wvmetronews.com Author:
Article Title: Princeton hospital to replace 12-hundred computer hard drives after cyber attack
Article URL: http://wvmetronews.com/2017/06/30/princeton-hospital-to-replace-computer-hard-drives-after-cyber-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170713-01	**YMCA San Diego**	CA	7/13/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On or about June 14, 2017, the YMCA became aware that an Excel spreadsheet containing personal information of certain YMCA employees was inadvertently sent over email to certain YMCA employees. While our investigation is ongoing, we determined the employee information contained in the Excel spreadsheet included: first and last name; Social Security number; address; date of birth; phone number; salary; former/maiden name; and disability code.

Attribution 1 Publication: CA AG's office Author:
Article Title: YMCA San Diego
Article URL: https://oag.ca.gov/system/files/YMCA%20-notice%20only_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170711-03	Movement Mortgage, LLC	SC	7/11/2017	Electronic	Banking/Credit/Financial	Yes - Published #	9,591

On September 8, 2016, Movement became aware of suspicious logins to certain company email accounts by an unknown source as the result of sophisticated phishing attacks on its email system. Movement's investigation determined that data relating to your personal information was stored within an affected company email account at the time unauthorized log-in's to that account occurred, including your <<ClientDef1>> <<ClientDef2>> (name, Social Security number, driver's license or state identification card number, bank account number, and payment card information, including card number, expiration date, and card security code)) (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NH AG' Author:
Article Title: Movement Mortgage, LLC
Article URL: https://oag.ca.gov/system/files/Movement%20Mortgage%20notice%20only5_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170711-02	Offices of Dr. Douglas Boucher, DDS and Dr. Andrea	CA	7/10/2017	Electronic	Medical/Healthcare	Yes - Published #	1,200

On June 2, 2017 our office received a ransomware notice from someone who had hacked our computer systems. The hacker did access our email system and may have accessed our patient dental health records.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
Article Title: Offices of Dr. Douglas Boucher, DDS and Dr. Andrea Yaley, DDS
Article URL: https://oag.ca.gov/system/files/Breach%20notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170711-01	University of California Davis Health	CA	7/5/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Recently, we discovered that an employee's work email account was accessed by an unknown third party on May 17, 2017. An email in this account contained the following information about you: name, address, and diagnosis.

Attribution 1 Publication: CA AG's Office Author:
Article Title: University of California Davis Health
Article URL: https://oag.ca.gov/system/files/BREACH_NOTIFICATION_SAMPLE_LETTER_AG_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170710-02	California Association of Realtors / Real Estate	CA	7/10/2017	Electronic	Business	Yes - Published #	1,000

The subsidiary, Real Estate Business Services (REBS), said malware was injected into the organization's online payment system at store.car.org and was active between March 13, 2017 and May 15, 2017, according to the San Diego Union Tribune. REBS sells educational material, products and forms to the association's members.

Attribution 1 Publication: scmagazine.com / CA AG's office Author:
Article Title: Data Breach hits California Association of Realtors
Article URL: https://www.scmagazine.com/data-breach-hits-california-association-of-realtors/article/673795/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170710-01	Avanti Markets	WA	7/8/2017	Electronic	Business	Yes - Published #	1,600,000

Avanti Markets, a company whose self-service payment kiosks sit beside shelves of snacks and drinks in thousands of corporate breakrooms across America, has suffered of breach of its internal networks in which hackers were able to push malicious software out to those payment devices, the company has acknowledged.

Attribution 1 Publication: krebsonsecurity.com / OR AG's office / Author:
Article Title: Self-Service Food Kiosk Vendor Avanti Hacked
Article URL: https://krebsonsecurity.com/2017/07/self-service-food-kiosk-vendor-avanti-hacked/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-13	UC Davis Health	CA	7/6/2017	Electronic	Medical/Healthcare	Yes - Published #	14,900

UC Davis Health is notifying approximately 15,000 patients of a security breach after an employee fell prey to an email phishing scam.

Attribution 1 Publication: sacramento.cbslocal.com / hipaajournal. Author:
Article Title: Email Phishing Scam Causes UC Davis Health Data Breach
Article URL: http://sacramento.cbslocal.com/2017/07/06/email-phishing-scam-leads-to-uc-davis-health-data-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-12	World Wrestling Entertainment, Inc. (WWE)	CT	7/7/2017	Electronic	Business	Yes - Unknown #	Unknown

The personal information of approximatley 3 million WWE website users was stored on an unprotected Amazon Web Services server, leaving them accessible to anyone who happened to stumble across them, according to Forbes. One included home and email addresses, birthdates, and the age ranges and genders of the account holders' children, he told Forbes. The other database contained addresses, telephone numbers, and names of WWE account holders in Europe.

Attribution 1 Publication: popculture.com / pcmag.com / esecurity Author:
Article Title: WWE Data Breach Exposes 3 Million Accounts
Article URL: https://www.pcmag.com/news/354817/wwe-data-breach-exposes-3-million-accounts

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-11	Atchafalaya Internal Medicine Associates	LA	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	2,000

Atchafalaya Internal Medicine Associates LA Healthcare Provider 2000 06/22/2017 Hacking/IT Incident Desktop Computer, Electronic Medical Record, Email, Laptop, Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: Atchafalaya Internal Medicine Associates
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=379466C9059D1E0C738000248BB64161

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-10	Pacific Ocean Pediatrics	CA	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	18,637

Pacific Ocean Pediatrics CA Healthcare Provider 18637 05/15/2017 Theft Other Portable Electronic Device

Attribution 1 Publication: hhs.gov Author:
Article Title: Pacific Ocean Pediatrics
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=379466C9059D1E0C738000248BB64161

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-09	Adams Industries, Inc.	NE	7/1/2017	Electronic	Business	Yes - Published #	647

Adams Industries, Inc. NE Health Plan 647 06/21/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Adams Industries, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=379466C9059D1E0C738000248BB64161

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-08	University of Iowa Hospitals & Clinics	IA	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	5,292

Iowa City-based University of Iowa Health Care notified patients June 22 after it discovered protected health information for roughly 5,300 had been available online for almost two years, the hospital confirmed to Becker's. Hospital officials said there is no indication any information — which included patient names, dates of admission and medical record numbers — was misused or "further disclosed."

Attribution 1 Publication: hhs.gov / Beckershospitalreview.com Author:
Article Title: University of Iowa Health Care discovers 5.3k patients' information exposed online for 2 years
Article URL: http://www.beckershospitalreview.com/healthcare-information-technology/5-3k-affected-when-iowa-hospital-discovers

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-06	**Enterprise Services LLC #1**	IN	7/1/2017	Electronic	Business	Yes - Published #	**56,075**

Enterprise Services LLC IN Business Associate 56075 06/27/2017 Unauthorized Access/Disclosure Network Server, Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Enterprise Services LLC #1
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=379466C9059D1E0C738000248BB64161

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-05	**Enterprise Services LLC (#2)**	CO	7/1/2017	Electronic	Business	Yes - Published #	**822**

Enterprise Services LLC CO Business Associate 822 06/30/2017 Unauthorized Access/Disclosure Network Server, Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Enterprise Services LLC (#2)
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=379466C9059D1E0C738000248BB64161

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-04	**GI Care for Kids Endoscopy Center**	GA	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,700**

A forensic investigation by third-party security experts found no evidence of data access or theft, with the investigators believing the attackers only used the ransomware to encrypt patient records in order to extort money from the company. While the attackers are not believed to have stolen or viewed data, the possibility could not be totally ruled out.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: GI Care for Kids Endoscopy Center Suffers Ransomware Attack
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=379466C9059D1E0C738000248BB64161

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-03	**Baptist Medical Center South**	FL	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	**531**

Baptist Medical Center South of Jacksonville, Florida has discovered a backup drive containing the electronic protected health information of 531 patients has gone missing.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Lost Backup Drive Contained PHI of More than 500 EEG Patients
Article URL: http://www.hipaajournal.com/lost-backup-drive-contained-phi-500-eeg-patients-8877/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-02	**PVHS-ICM Employee Health and Wellness, LLC**	CO	7/1/2017	Electronic	Medical/Healthcare	Yes - Published #	**10,143**

Ransomware was installed on a server at a single UCHealth walk-in clinic in Fort Collins, CO. The ransomware attack was discovered on May 4, 2017, with the crypto-ransomware believed to have been installed the same day. The protected health information on the server included patients' names, home addresses and other demographic information along with health records, including diagnoses and treatment information. Some patients' Social Security numbers were also stored on the server.

Attribution 1 Publication: hhs.gov / hipaajournal.com / VT AG's off Author:
Article Title: Almost 12,000 Records Compromised in Two New Ransomware Attacks
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=379466C9059D1E0C738000248BB64161

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170707-01	**B&B Theaters**	MO	7/1/2017	Electronic	Business	Yes - Published #	**1,133**

"While some malware was identified on B&B systems that dated back to 2015, the investigation completed by Trustwave did not conclude that customer data was at risk on all B&B systems for the entirety of the breach." (Exposure number per NY AG's office / notification from Discover)

Attribution 1 Publication: krebsonsecurity.com / NY AG's office Author:
Article Title: B&B Theatres Hit in 2-Year Credit Card Breach
Article URL: https://krebsonsecurity.com/2017/07/bb-theatres-hit-in-2-year-credit-card-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170706-03	**Indiana Health Coverage Program / DXC Technology**	IN	7/1/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

The fiscal agent for the Indiana Health Coverage Program (IHCP), DXC Technology, says a hyperlink to an IHCP report containing patient information was accessible online. The information exposed was limited to names, Medicaid ID numbers, patient numbers, procedure codes, dates of service, payment amounts and names/addresses of health care providers.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Indiana Medicaid Recipients Alerted to Potential Data Breach
Article URL: http://www.hipaajournal.com/indiana-medicaid-recipients-alerted-to-potential-data-breach-8877/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170706-02	**Meepos & Co.**	CA	7/1/2017	Electronic	Business	Yes - Published #	**1,910**

Through the investigation, Meepos determined that an unauthorized actor or actors gained access to certain parts of Meepos's network due to a misconfiguration of our two-factor password authentication and, as a result, may have had access to personal information for certain Meepos clients in our tax filing system, including documents that may be associated with our business client tax filings. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MD AG's office / NY AG Author:
Article Title: Meepos & Co.
Article URL: https://oag.ca.gov/system/files/Meepos%20-%20notice%20only_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170706-01	**White Blossom Care Center**	CA	7/1/2017	Electronic	Business	Yes - Published #	**800**

On May 25, 2017, we received information that a former White Blossom employee may have improperly accessed resident data while employed at the facility. We currently believe that a limited number of the inappropriately acquired files contained some combination of resident names with social security numbers, dates of birth, health insurance carrier and account numbers, and/or limited medical information, such as admission dates, diagnoses, medications, and/or procedures.

Attribution 1 Publication: CA AG's office / hipaajournal.com Author:
Article Title: White Blossom Care Center
Article URL: https://oag.ca.gov/system/files/S027_v05.pdf_Resident%20Notice%20FINAL_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-13	**RJD, LLC dba Guardian Technologies, LLC**	OH	6/7/2017	Electronic	Business	Yes - Unknown #	**Unknown**

It is our understanding that on April 26, 2017, Guardian learned it may have been the victim of a cyber-attack. The potentially compromised information includes customer names, e-mail addresses, mailing addresses, and payment information, including credit card information.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: RJD, LLC dba Guardian Technologies, LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/rjd-20170607.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-12	Leader Bank	MA	6/6/2017	Electronic	Banking/Credit/Financial	Yes - Published #	362

As the result of an intensive review of ZRent's files , servers and coding, as well as IP address access and account activity, Leader Bank determined that on December 30, 2016, a malicious actor was able to exploit the "upload picture" feature and upload a malicious file to the ZRent server. Thus, the landlords who had established a ZRent account prior to May 19, 2017 may have had their bank account numbers, dates of birth (if provided) and social security or tax identification numbers
(if provided) compromised. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: Leader Bank
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/leader-bank-20170607.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-11	Karp, Ackerman, Skabowski & Hogan, CPAs PC	NY	6/27/2017	Electronic	Business	Yes - Published #	256

On or about May 26, 2017, KASH discovered that certain of your personal information may have been affected when an external actor is believed to have gained access to a limited number of electronic tax files. We believe that those files contained certain of your personal information, including your name, address and Social Security number. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Karp, Ackerman, Skabowski & Hogan, CPAs PC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/karp-ackerman-skabowski-hogan-20170627.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-10	First National Bank of Pennsylvania (5/26)	PA	5/26/2017	Electronic	Banking/Credit/Financial	Yes - Published #	6,718

On or about January 23, 2017, FNB learned of a suspicious email message that was received by an FNB employee on January 10, 2017. While our investigation is ongoing, we determined on April 27, 2017, that one or more of the following types of information related to you may have been contained in a message or attachment in the affected email account and may have been accessible to the unauthorized and unknown individual(s): name, address, Social Security number, driver's license number, credit card number and/or financial account number. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: First National Bank of Pennsylvania (5/26)
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/first-national-bank-pennsylvania-20170526.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-09	Burdette Smith & Bish	VA	6/26/2017	Electronic	Business	Yes - Published #	1,285

Our investigation determined that an unauthorized individual accessed the server beginning on March 23, 2017, and the server contained files that may have included your name, date of birth, address, social security number, and tax or financial information such as tax returns, W-2s, 1095s, and for some individuals, credit card and bank statements. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / VT AG's office / NY AG' Author:
Article Title: Burdette Smith & Bish
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/burdette-smith-bish-20170626.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-08	Office of Elizabeth L. Brown, MD, PLLC	WV	5/12/2017	Electronic	Medical/Healthcare	Yes - Published #	8,436

Elizabeth L. Brown, MD, PLLC WV Healthcare Provider 8436 05/12/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Elizabeth L. Brown, MD, PLLC
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=B0217CDBB07B75E7CFC92C7657E870CC

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-07	Condie Stoker & Associates	ID	6/16/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 18, 2017, the extensive forensic investigation concluded that an unauthorized third party may have had access to our systems on or about January 3, 2017 and, as a result, obtained certain client
information. The information affected by this incident includes your full name, date of birth, address, and Social Security number, and may also include your email address.

Attribution 1 Publication: MT AG's office Author:
Article Title: Condie Stoker & Associates
Article URL: https://dojmt.gov/wp-content/uploads/Condie-Stoker.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-06	Xtant Medical	MT	6/30/2017	Electronic	Business	Yes - Unknown #	Unknown

On June 2, 2017 we learned that an e-mail account belonging to one of our employees was compromised and accessed by an unknown third party on or about June 1, 2017. During our investigation into thecompromise, we learned that the account held your W-9 Form and/or certain bank account information at the time it was accessed.

Attribution 1 Publication: MT AG's office / MD AG's office / NY AG Author:
Article Title: Xtant Medical
Article URL: https://dojmt.gov/wp-content/uploads/Xtant-Medical-Holdings.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-05	Michael A. Adams, CPA	CA	6/30/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 31, 2017, my locked vehicle was broken into and my password protected laptop was stolen. The information may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (potentially including the last four digits of the account number), and direct deposit bank account information for refunds or payments (including account number and routing information if provided to me).

Attribution 1 Publication: MT AG's office Author:
Article Title: Michael A. Adams, CPA
Article URL: https://dojmt.gov/wp-content/uploads/Epiq.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-04	State Farm Mutual Automobile Insurance	IL	6/29/2017	Electronic	Business	Yes - Unknown #	Unknown

Recently, State Farm became aware that an unauthorized online enablement to your accounts on statefarm.com had occurred. Our investigation identified unauthorized activity including the misuse of your financial card, and the alteration of your contact information. Your personal information which may have been accessed included your name, contact information, insurance policy information, social security number, driver's license number and financial card number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-03	U.S. Cellular	IL	6/22/2017	Electronic	Business	Yes - Published #	1,852

It appears that your My Account has been accessed by hackers as a result of this attack. As indicated above, your user name and password which were used to access your My Account have been compromised. Your My Account contains your Social Security number, name, address, and cellular telephone number(s) as well as information about your wireless services including your service plan, usage and billing statements known as Customer Proprietary Network Information ("CPNI"). (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / MD A Author:
Article Title: U.S. Cellular
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/us-cellular-20171024.pdf

Attribution 2 Publication: VT AG's office / WI AG's office Author:
Article Title: U.S. Cellular
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/United%20States%20Cellular%20Corporation%20SBN

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-02	**County Commissioners Association of Pennsylvania /**	PA	6/30/2017	Electronic	Business	Yes - Published #	**1,800**

Approximately 1,800 children had their identities compromised in a data security breach, including 186 in the region, according to the County Commissioners Association of Pennsylvania. Officials said Thursday that a Pennsylvania-based Children and Youth Services caseworker found a link on the internet to a client file. Authorities said the information may have included personal identifiable information and personal health information.

Attribution 1 Publication: databreaches.net / wjactv.com Author:
Article Title: Officials: Nearly 200 children in region affected by data security breach
Article URL: http://wjactv.com/news/local/officials-nearly-200-children-in-region-affected-by-security-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170630-01	**Professional Counseling and Medical Associates**	TN	6/30/2017	Electronic	Medical/Healthcare	Yes - Published #	**2,500**

Professional Counseling and Medical Associates, 849 Volunteer Dr., Suite 2, reported a breach of its electronic health records system, which was copied by a disgruntled former employee who is a healthcare professional.

Attribution 1 Publication: databreaches.net / parispi.net / hhs.gov Author:
Article Title: Clinic tells patients about records theft
Article URL: http://www.parispi.net/news/local_news/article_abaa018c-5d3a-11e7-bdcf-bb24fa55547f.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170629-02	**Paul Stuart, Inc.**	NY	6/29/2017	Electronic	Business	Yes - Published #	**6,477**

On May 15, 2017, we learned that an unknown individual may have accessed your credit or debit card information used to make purchases at our online store. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NH AG' Author:
Article Title: Paul Stuart, Inc.
Article URL: https://oag.ca.gov/system/files/Paul%20Stuart%20notice%20only_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170629-01	**8tracks Radio**	CA	6/29/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Hackers accessed 8tracks's user database and pilfered information, including email addresses and encrypted passwords, from at least 18 million accounts signed up for the Internet radio service using email.
“If you signed up via Google or Facebook authentication, then your password is not affected by this leak,” according to a Tuesday blog post on the company's website.

Attribution 1 Publication: scmagazine.com Author:
Article Title: 8tracks breach yields data on 18M accounts
Article URL: https://www.scmagazine.com/8tracks-breach-yields-data-on-18m-accounts/article/672233/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170627-06	**Texas Association of School Boards (TASB)**	TX	6/27/2017	Electronic	Educational	Yes - Published #	**6,100**

Last week Laredo ISD employees were notified that there was a security breach involving very important information about its employees. As of right now, the district is not sure when the breach happened, but they know that the names and social security numbers of some LISD’s employees were made public on a website by the Texas Association of School boards. Includes: Laredo ISD, Corpus Christi ISD, Alief SD, Callelen ISD, Victoria School District

Attribution 1 Publication: databreaches.net / KGNS.com Author:
Article Title: Texas Association of School Boards data breach exposed thousands of teachers' SSNs
Article URL: https://www.databreaches.net/texas-association-of-school-boards-data-breach-exposed-thousands-of-teachers-ssns/

Attribution 2 Publication: caller.com Author:
Article Title: CCISD: employee information inadvertently made visible online
Article URL: http://www.caller.com/story/news/education/2017/06/21/ccisd-employee-information-inadvertently-made-visible-online/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170627-05	Orthodontic Specialists of Green Bay	WI	4/24/2017	Electronic	Medical/Healthcare	Yes - Published #	742

Orthodontic Specialists of Green Bay WI Healthcare Provider 742 04/24/2017 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Orthodontic Specialists of Green Bay
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=5EF15A7D70BE8C373015B10443413BD9

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170627-04	Advanced ENT Head & Neck Surgery	CA	5/31/2017	Electronic	Medical/Healthcare	Yes - Published #	15,000

Advanced ENT Head & Neck Surgery CA Healthcare Provider 15000 05/31/2017 Theft Desktop Computer, Electronic Medical Record, Email, Laptop, Other, Other Portable Electronic Device, Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Advanced ENT Head & Neck Surgery
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=5EF15A7D70BE8C373015B10443413BD9

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170627-03	Family Tree Health Clinic	TX	6/19/2017	Electronic	Medical/Healthcare	Yes - Published #	13,402

On April 24, 2017, Family Tree Health Clinic, P.A. ("Family Tree") discovered that cyber attackers gained unauthorized access to its IT systems by executing a sophisticated, ransomware-encryption attack. Our system data was restored from backups and no ransom was paid to the cyber criminals. The systems accessed by this attack may have included names, date of birth, address, Social Security number, health insurance information and medical information such as claims and diagnosis codes. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / hipaajournjal.com / MD Author:
Article Title: Family Tree Health Clinic
Article URL: https://dojmt.gov/wp-content/uploads/Family-Tree-Health-Clinic.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170627-02	Experian Health (other health systems)	TN	6/27/2017	Electronic	Medical/Healthcare	Yes - Published #	727

Experian Health has discovered the protected health information of some patients has been accidentally disclosed to incorrect individuals due to a technical error that occurred during a server migration. The disclosed data including names, addresses, genders, dates of birth, Medicare ID/HIC numbers, member ID numbers, insurance/payer company names, group numbers/group policy numbers and Medicaid case numbers. The data were shared with incorrect HIPAA covered entities.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Cook County Health and Hospitals System Patients Impacted by Experian Health Breach
Article URL: https://www.hipaajournal.com/cook-county-health-and-hospitals-system-experian-health-breach/

Attribution 2 Publication: hipaajournal.com Author:
Article Title: Experian Health Accidentally Sends PHI to Incorrect Individuals
Article URL: http://www.hipaajournal.com/experian-health-accidentally-sends-phi-to-incorrect-individuals-8864/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170627-01	**GOLFTEC**	CO	6/16/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We experienced malicious point-of-sale terminal intrusions at select GOLFTEC centers from March 2 – June 15, 2017. You are receiving this letter because GOLFTEC was victim of a recent security breach at your specific GOLFTEC Center and your credit card information was potentially compromised.

Attribution 1 Publication: CA AG's office / MD AG's pffice Author:
Article Title: GOLFTEC
Article URL: https://oag.ca.gov/system/files/GOLFTEC-Security%20Breach%20Letter%20%286.14.17%29-California%20Version_0.p

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-12	**David Turrentine & Associates, Inc.**	IL	6/20/2017	Electronic	Business	Yes - Published #	**1,948**

On or about March 30, 2017, I became aware that David Turrentine & Associates, Inc. may have been the victim of a cyber-attack by which an unknown third party was able to access my firm's computer network and some of my clients' personal information. Based on the internal investigation of this matter, the client information potentially at risk of being accessed included first and last names, home addresses, social security numbers, and 2015 tax return information, including compensation data. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: David Turrentine & Associates, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/turrentine-20170620.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-11	**Santander Bank (5/22)**	MA	6/19/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**434**

On May 25, 2017, the Santander Bank Fraud Risk group identified an ATM skimming event at a Santander Bank ATM terminal in Billerica MA. The personal information potentially compromised included the customer's name, card number, card expiration date, card security code, and card PIN number. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Santander Bank (5/22)
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/santander-20170619.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-10	**Parkhurst Dining**	PA	6/13/2017	Electronic	Business	Yes - Published #	**572**

On April 20 2017, we learned that a Parkhurst Dining team member had clicked on a phishing email and entered their credentials. But, we have confirmed that your «ClientDef1 "Social Security number, date of birth, medical information, drivers license number, bank account number. benefits election form, benefits enrollment form, birth certificate, state identification number credit card number, and passport number">> were accessible to the unknown actor. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / CT AG's office / MD AG Author:
Article Title: Parkhurst Dining
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/parkhurst-dining-20170613.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-09	**Toth Enterprises II dba Victory Medical**	TX	6/5/2017	Electronic	Medical/Healthcare	Yes - Published #	**2,000**

Toth Enterprises II d/b/a Victory Medical TX Healthcare Provider 2000 06/05/2017 Unauthorized Access/Disclosure Email, Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Toth Enterprises II dba Victory Medical
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=F7F8B8C8116C16A7EE5C3351967E0CFF

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-08	**Missouri Department of Mental Health**	MO	2/7/2017	Electronic	Government/Military	Yes - Published #	**5,685**

Mo. Dept. of Mental Health MO Healthcare Provider 5685 02/07/2017 Hacking/IT Incident Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Missouri Department of Mental 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
ITRC20170623-07	**Waverly Health Center**	IA	6/20/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

On June 14, 2017 an unknown ransomware variant infected the Waverly Health Center, a hospital located in Waverly, Iowa. Fortunately, the facility encrypts all of their patient data. Therefore, the hackers were unable to obtain any of the patient's personal information.

Attribution 1 Publication: databreaches.net / techtalk. Author:
Article Title: Midwestern Hospital Infected With Ransomware
Article URL: http://techtalk.pcpitstop.com/2017/06/19/iowan-hospital-infected-ransomware/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-06	**Miami-Dade County Public Schools**	FL	6/20/2017	Electronic	Educational	Yes - Published #	**522**

Two former Miami-Dade school students claim the Miami-Dade County School Board was reckless and negligent for publishing students' private information on the Miami-Dade County Public Schools (MDCPS) website.nformation such as social security number, developmental scale score, whether they passed or failed the FCAT, achievement levels and other test scores.

Attribution 1 Publication: databreaches.net / miami.cbslocal.com Author:
Article Title: Former MDCPS Students Suing School Board Over Publishing Of Private Info
Article URL: http://miami.cbslocal.com/2017/06/20/student-sue-miami-dade-county-school-board-private-information/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-05	**Cleveland Medical Associates**	TN	6/22/2017	Electronic	Medical/Healthcare	Yes - Published #	**22,000**

Cleveland Medical Associates, PLLC, a four-physician primary care clinic in Cleveland, Tennessee, is providing notice to its patients that on April 21, 2017, it discovered that, the evening before, its computer network had been impacted by ransomware, a type of computer virus that locks up, or encrypts, information and demands that a payment be made in order to unlock, or decrypt, the information.

Attribution 1 Publication: databreaches.net / hipaajournal.com Author:
Article Title: Cleveland Medical Associates tells patients of ransomware incident
Article URL: https://www.databreaches.net/cleveland-medical-associates-tells-patients-of-ransomware-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-04	**Aetna / Bayer Corporation**	CT	6/21/2017	Electronic	Medical/Healthcare	Yes - Published #	**5,002**

On April 27, 2017, Aetna became aware of a concern involving two Aetna web services used to display plan-related documents to members and other intended recipients. Aetna determined that the information cataloged by the search engines generally included member names, Aetna member identification numbers, provider information, claim payment amounts, and in some cases procedure/service codes and dates of service.

Attribution 1 Publication: MT AG's office / hipaajournal.com / NY Author:
Article Title: Aetna / Bayer Corporation
Article URL: https://dojmt.gov/wp-content/uploads/Aetna-1.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-03	**St. Thomas Rutherford Hospital**	TN	6/22/2017	Paper Data	Medical/Healthcare	Yes - Published #	**2,859**

Today, another HIPAA-covered entity – Saint Thomas Rutherford Hospital in Murfreesboro, TN – has reported a similar incident. Documents containing the protected health information of almost 3,000 patients were discovered to have been abandoned by the side of a remote, rural road in DeKalb County in April.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 2,859 Patients Impacted by Improper Disposal at St. Thomas Rutherford Hospital
Article URL: http://www.hipaajournal.com/2859-patients-impacted-improper-disposal-st-thomas-rutherford-hospital-8856/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-02	**Caliber Home Loans, Inc.**	TX	6/22/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

Based upon extensive investigation conducted by a leading forensic firm, it appears that beginning on approximately January 18, 2017, unauthorized individuals gained the ability to access a limited number of electronically-stored loan files, and may have had access to other documents containing personally-identifying information. The files and documents that were subject to unauthorized access may have contained certain customers' sensitive or identifying information, such as social security number, driver's license number, military or other government ID number, or date of birth; financial account names, numbers, and statements; digital signatures, and/or information that an individual may be able to use to access a customer's online Caliber account or data storage sites containing borrower submissions.

Attribution 1 Publication: CA AG's office / MT AG's office / MD AG Author:
Article Title: Caliber Home Loans, Inc.
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_11.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170623-01	**Home Point Financial Corporation**	CA	6/20/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**32,642**

On March 30, 2017, we learned that an unauthorized individual utilized a phishing scheme and may have gained access to employees' email accounts beginning in November 2016. We conducted a thorough review of the employees' email accounts and determined that they contained information that you may have included with your loan application such as your name, address, Social Security number, date of birth, driver's license/passport/state identification number, payment card number, and financial account numbers. (Exposure number per NY AG's office

Attribution 1 Publication: CA AG's office / OR AG's office / NH AG Author:
Article Title: Home Point Financial Corporation
Article URL: https://oag.ca.gov/system/files/ca%20notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170620-02	**Yeo & Yeo CPAs & Business Consultants**	MI	6/12/2017	Electronic	Business	Yes - Published #	**3,491**

Our investigation determined that your 2015 tax information was accessed by unauthorized individual(s). The information contained in the tax returns included your name, address, and Social Security number. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NY AG's office / MD AG' Author:
Article Title: Yeo & Yeo CPAs & Business Consultants
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Yeo%20&%20Yeo%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170620-01	**Torrance Memorial Medical Center**	CA	6/19/2017	Electronic	Medical/Healthcare	Yes - Published #	**46,632**

On April 20, 2017, Torrance Memorial Medical Center ("Torrance Memorial") discovered that it had experienced an email security incident that allowed access to staff members' email accounts which contained work-related reports. Based on the investigation, we have determined that the information affected may include your: name, Social Security number, address, health insurance information, date of birth, and treatment/diagnostic information. (Exposure number per HHS)

Attribution 1 Publication: CA AG'soffice / hipaajournal.com / MT A Author:
Article Title: Torrance Memorial Medical Center
Article URL: https://oag.ca.gov/system/files/Torrance%20-%20notice%20only_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170619-05	Occidental College	CA	6/1/2017	Electronic	Educational	Yes - Unknown #	Unknown

The college has reason to believe that on or around June 1, 2017, an unauthorized person may have gained access to a computer file containing a limited amount of personally identifiable information. The file in question included names, Oxy ID numbers and associated encoded data that enables Oxy ID cards to function as on-campus debit cards. The file did NOT include Social Security numbers, driver's license or other state-issued ID numbers, financial information (such as credit card or banking information), or other sensitive personal data. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / MD AG Author:
Article Title: Occidental College
Article URL: https://oag.ca.gov/system/files/20170619%20Occidental%20College%20Sample%20Notice-CA_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170619-04	Little River Healthcare	TX	6/16/2017	Paper Data	Medical/Healthcare	Yes - Published #	542

Little River Healthcare discovered May 12 that a briefcase containing 18 paper charts and a laptop with patient electronic medical records, was stolen from a provider's locked vehicle. Among the information stolen was: patient names, dates of birth, dates of service, and medical history. The records did not include social security numbers, driver's license numbers or patient home addresses.

Attribution 1 Publication: databreaches.net / kcentv.com / MT AG' Author:
Article Title: Briefcase containing Little River Healthcare records stolen
Article URL: http://www.kcentv.com/news/local/briefcase-containing-little-river-healthcare-records-stolen/449836151

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170619-03	Deep Root Analytics / Republican National	VA	6/19/2017	Electronic	Business	Yes - Unknown #	Unknown

Information of nearly 200 million registered voters compiled for the Republican National Committee (RNC) was exposed on a database and accessible without a password, according to a story in The Hill. UpGuard, the security firm which detected the security vulnerability, attributed the leak to a misconfigured database managed by Deep Root Analytics (DRA), a data analytics firm contracted by the Republican party during the presidential campaign.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Data of 200M voters exposed via RNC contractor
Article URL: https://www.scmagazine.com/data-of-200m-voters-exposed-via-rnc-contractor/article/669411/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170619-02	Buckle Inc.	NE	6/19/2017	Electronic	Business	Yes - Published #	1,993

Buckle Inc. was hit with point-of-sale (POS) malware on the payment data systems at an undisclosed number of locations.The malware searched for track data read from the magnetic stripe of a payment card and was designed to steal payment card data including account numbers, account holder names, and expiration dates, according to a June 16 press release. (Exposure number per NY AG's office per notification from Discover)

Attribution 1 Publication: scmagazine.com / OR AG's office / NY Author:
Article Title: POS breach hits Buckle Inc. stores
Article URL: https://www.scmagazine.com/buckle-clothier-stores-hit-with-pos-malware/article/669416/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170619-01	Bed Bath & Beyond	NJ	5/15/2017	Electronic	Business	Yes - Unknown #	Unknown

We detected recent irregular activity on our website that suggests that your Bed Bath & Beyond online account may have been compromised.Depending on how you have your account set up and what information you have elected to save, that basic account information may include your name, email address, phone number, default shipping, billing, and mailing address, and/or the card type, expiration date, and last four digits of the card number for any credit or debit card that you saved on your account. It would not have included the full credit card number or the security code on any card.

Attribution 1 Publication: CA AG's office / WI AG's office Author:
Article Title: Bed Bath & Beyond
Article URL: https://oag.ca.gov/system/files/Bed%20Bath%20%26%20Beyond%20--%20CA%20attachments_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-13	Texas Health and Human Services	TX	6/16/2017	Paper Data	Government/Military	Yes - Published #	1,842

The Health and Human Services Commission is notifying people about the accidental loss of protected personal information. The breach may affect 1,842 people in the Houston area. Other potential information includes mailing addresses, Social Security numbers, health information and bank account numbers.

Attribution 1 Publication: cw39.com / hhs.gov Author:
Article Title: Officials announce data breach after more than 1,800 patient health documents found near dumpster
Article URL: http://cw39.com/2017/06/16/officials-announce-data-breach-after-more-than-1800-patient-health-documents-found-near

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-12	Provident Credit Union	CA	6/13/2017	Electronic	Banking/Credit/Financial	Yes - Published #	192

On April 25, 2017, Providenl confirmed that certain of ycur personal information (described below) may have been disclosed by a former employee of Creditors Specialty Services, Inc. ("CSS") on or about March 3, 2017. Provident believes that your personal information involved in this incident may include your name, home address and Social Security number. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Provident Credit Union
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/provident-credit-20170613.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-11	Pioneer Valley Books	MA	6/12/2017	Electronic	Business	Yes - Published #	929

PVB has learned that an unauthorized intruder may have gained entry to its web server and installed malicious computer code designed to steal credit card information. Your name, email address, and credit card information, along with the security code for your card, may have been acquired. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / MD AG' Author:
Article Title: Pioneer Valley Books
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Pioneer%20Valley%20Books%20SBN%20to%20Consu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-10	O'Brien Riley & Ryan, P.C.	MA	6/8/2017	Electronic	Business	Yes - Published #	181

On April 28, 2017 we discovered that earlier that day, as a result of a criminal phishing email, an unauthorized third party obtained access to electronic files containing tax documents, including W-2s, of some of O'Brien Riley & Ryan, P.C's clients' employees. We have confirmed that the information obtained by the unauthorized party included your W-2, which included your full name, Social Security number, home address, and wage and tax withholding information. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / MD AG's office / NY AG' Author:
Article Title: O'Brien Riley & Ryan, P.C.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/O'Brien%20Riley%20&%20Ryan,%20P.C.%20SBN%20t

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-09	Scatco Abstracts & Title Insurance / Three Rivers Title	AR	6/16/2017	Paper Data	Business	Yes - Published #	200

Greenwood police are investigating after nearly a dozen folders of paperwork containing personal information were found in the middle of a busy street. "We started picking up the paperwork and noticed it was mortgage information with social security numbers, dates of birth and even banking information," Bowling said. "We knew right then and there, it was sensitive information and we tried to gather up as much as we could and try to get it secure."

Attribution 1 Publication: databreaches.net / 5newsonline.com Author:
Article Title: Hundreds Of Files With Personal Information Found In Greenwood
Article URL: http://5newsonline.com/2017/06/15/hundreds-of-files-with-personal-information-found-in-greenwood/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-08	Union Bank & Trust (UBT)	NE	6/15/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Our website experienced a data security breach which may have compromised the personal information of some of our clients. This information would have included names, billing and shipping addresses, email addresses, credit card numbers, CVV ("Card Verification Value") numbers, credit card expiration dates, and website passwords.

Attribution 1 Publication: MT AG's office Author:
Article Title: Union Bank & Trust (UBT)
Article URL: https://dojmt.gov/wp-content/uploads/UBT.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-07	Leavitt Group	UT	6/12/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 29, 2017, it came to our attention that certain members of our staff received phishing emails to their Leavitt email accounts. While our investigation is ongoing, we have determined an email sent to us on [date] containing the names and driver's license numbers of ## members of your staff was accessed by the unknown intruder.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-06	Cove Family and Sports Medicine / Krichev Family	AL	6/13/2017	Electronic	Medical/Healthcare	Yes - Published #	4,300

On Aprill4, 2017, Cove Medicine's computer system was infected by a ransomware virus that encrypted our electronic medical software containing our patients' medical records.

Attribution 1 Publication: MT AG's office / hhs.gov / hipaajournal.c Author:
Article Title: Cove Family and Sports Medicine / Krichev Family Medicine, P.C
Article URL: https://dojmt.gov/wp-content/uploads/Cove-Family-Sports-Medicine.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-05	Forum for Youth Investment	DC	6/8/2017	Electronic	Business	Yes - Published #	643

On March 27, 2017, we discovered that the Forum for Youth Investment was the victim of a ransomware attack. What Information Was Involved? Our investigation has determined that the information contained on the affected system included your <<data elements list>> and name. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / CT AG's office / MD AG Author:
Article Title: Forum for Youth Investment
Article URL: https://dojmt.gov/wp-content/uploads/The-Forum-for-Youth-Investment.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-04	Onia LLC / Acadace, LLC	NY	6/7/2017	Electronic	Business	Yes - Unknown #	Unknown

On April 11, 2017, Onia's e-commerce service provider, Acadaca, LLC ("Acadaca") discovered evidence of malicious code on all pages of Onia's website. Acadaca has determined that the malware was present on Onia's website from November 12, 2016 to April 11, 2017 Consequently, the malware was able to capture personal and financial information related to e-commerce transactions using Onia's checkout process.

Attribution 1 Publication: MT AG's office / VT AG's office / MD AG' Author:
Article Title: Onia LLC
Article URL: https://dojmt.gov/wp-content/uploads/Onia.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-03	**Jewelry.com / Richline Group, Inc.**	FL	6/7/2017	Electronic	Business	Yes - Published #	**7,000**

On May 16, 2017 Jewelry.com discovered that, beginning on or about November 16, 2016, unknown individuals gained access to our online boutique through the unauthorized use of an account belonging to one of our employees. he compromised information includes debit and credit card numbers, card holders' names, card holders' billing addresses, passwords, security codes and expiration dates. (Richline Group, Inc.)

Attribution 1 Publication: MT AG's office / CA AG's office / NH AG' Author:
Article Title: Jewelry.com / Richline Group, Inc.
Article URL: https://dojmt.gov/wp-content/uploads/Jewelry.com_.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-02	**Southern Tide**	SC	6/15/2017	Electronic	Business	Yes - Published #	**4,315**

Based upon an extensive forensic investigation, it appears that an unauthorized individual gained access to portions of our website and placed malicious software that was designed to capture credit card or debit card information. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / VT AG's office / NH AG' Author:
Article Title: Southern Tide
Article URL: https://dojmt.gov/wp-content/uploads/Southern-Tide.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170616-01	**Sadd Velazquez Higashi Shamaa (SVHS)**	CA	6/15/2017	Electronic	Business	Yes - Published #	**4,625**

On June 8, 2017, the specialized forensic IT firm determined that there was unauthorized access to our system on May 1 through May 3, 2017. This information may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), and direct deposit bank account information (including account number and routing information if provided to us). (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / CA AG's office / NH AG' Author:
Article Title: Sadd Velazquez Higashi Shamaa
Article URL: https://dojmt.gov/wp-content/uploads/SVHS.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170615-05	**CCHI Insurance Services**	CA	6/1/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,000**

CCHI Insurance Services CA Health Plan 1000 06/01/2017 Theft Desktop Computer, Electronic Medical Record, Email, Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: CCHI Insurance Services
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=E5404152B9B7DA5BA4CE7F5E5E743C47

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170615-04	**Tennessee Rural Health Improvement Association**	TN	6/8/2017	Paper Data	Business	Yes - Published #	**588**

Tennessee Rural Health Improvement Association TN Health Plan 588 06/08/2017 Loss Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Tennessee Rural Health Improvement Association
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=E5404152B9B7DA5BA4CE7F5E5E743C47

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170615-03	**Durango Family Medicine**	CO	6/15/2017	Electronic	Medical/Healthcare	Yes - Published #	**18,790**

On June 6, Terry Cipoletti, an attorney with Caplan & Earnest LLC, sent out a letter about the security breach, saying Durango Family Medicine on April 7 discovered a portable external hard drive containing patient information was discovered missing from the medical office where it was stored. The type of information contained on the missing hard drive included electronic patient charts that contain: patient names and ID numbers, dates of birth, addresses, phone numbers, insurance carriers, dates of service and certain clinical information such as medical problem lists, vital signs, diagnoses and medical conditions, allergies, medications, progress notes, admission and discharge notes, operative report notes, lab and/or diagnostic study results, social histories, letters of referral and consultation notes.

Attribution 1 Publication: durangoherald.com / databreaches.net Author:
Article Title: Former Durango Family Medicine patients warned of security breach
Article URL: https://durangoherald.com/articles/165563-former-durango-family-medicine-patients-warned-of-security-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170615-02	**CashCrate**	ID	6/15/2017	Electronic	Business	Yes - Unknown #	**Unknown**

User data on six million subscribers to the cash-for-surveys site CashCrate has been compromised, according to a report on Motherboard. The company is blaming the breach on its third-party forum software, and is notifying customers, it informed Motherboard. Meanwhile, the software has been deactivated. User data going back 10 years – including email addresses, names, passwords and street addresses – was stolen in the breach.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Accounts of 6M CashCrate users exposed
Article URL: https://www.scmagazine.com/accounts-of-6m-cashcrate-users-exposed/article/668889/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170615-01	**Gracenote, a Nielsen Company**	CA	5/18/2017	Electronic	Business	Yes - Published #	**3,000**

A laptop belonging to a Gracenote employee was stolen from a vehicle in the California Bay Area on May 18, 2017. During the course of our investigation, we learned that the laptop may have contained personal information, including contact information (e.g., name, work email, address), as well as government identification numbers for current and former Gracenote associates. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / NY AG' Author:
Article Title: Gracenote
Article URL: https://oag.ca.gov/system/files/Nielsen%20Gracenote%20Ad%20r3prf.0615_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170614-02	**Oklahoma University**	OK	6/14/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

OU unintentionally exposed thousands of students' educational records — including social security numbers, financial aid information and grades in records dating to at least 2002 — through lax privacy settings in a campus file-sharing network, violating federal law.

Attribution 1 Publication: databreaches.net / OUDaily Author:
Article Title: Oklahoma U. shuts down file sharing service after failing to protect thousands of students' records
Article URL: https://www.databreaches.net/oklahoma-u-shuts-down-file-sharing-service-after-failing-to-protect-thousands-of-stude

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170614-01	**Bridge Investment Group**	UT	6/12/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**1,948**

We recently learned that an unauthorized individual was able to gain access to portions of the Bridge network and, while on the network, had the ability to access certain investor files stored there. Although the specific information maintained about particular investors varies from person to person, we believe that certain information, including first and last name, address, government identification information (such as driver's license or passport), Social Security number, financial account information, may be contained in these files and could be affected as a result of this incident. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office / MD AG Author:
Article Title: Bridge Investment Group
Article URL: https://dojmt.gov/wp-content/uploads/Bridge-Investment-Group.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170613-02	**N. Fred Eaglstein, D.O. dba Dermatology and Laser**	FL	5/30/2017	Electronic	Medical/Healthcare	Yes - Published #	**2,000**

N. Fred Eaglstein, D.O. d/b/a Dermatology and Laser Center FL Healthcare Provider 2000 05/30/2017 Unauthorized Access/Disclosure Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: Dermatology and Laser Center (Office of N. Fred Eaglstein, D.O.)
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170613-01	**Tutti Music Player Users / Spectrum Interactive**	NY	6/8/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We are unable to determine whether any user data was stolen by the third party at this time, but our system was subject to third party ransomware which encrypted server data. The server that was impacted by the attack included user email addresses and passwords stored by us. It did NOT include credit card information, DOB, or other personal identification numbers.

Attribution 1 Publication: OR AG's office Author:
Article Title: Tutti Music Player Users
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1589805587

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170612-01	**Washington State University - Social & Economic Sciences**	WA	6/9/2017	Electronic	Educational	Yes - Published #	**1,118,135**

On April 21, 2017, Washington State University learned that a locked safe containing a hard drive had been stolen. We know that not all of the information on the drive was encrypted and we have determined that the hard drive contained some of your personal information, including your name, address<variable data>. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office Author:
Article Title: Washington State University
Article URL: https://oag.ca.gov/system/files/WSU%20Notice%20Adult%20CA%20Sample_0.pdf?

Attribution 2 Publication: databreaches.net / WSU website / CA A Author:
Article Title: Washington State Uni notifies those affected by stolen hard drive
Article URL: https://www.databreaches.net/washington-state-uni-notifies-those-affected-by-stolen-hard-drive/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170608-03	**Southwest Community Health Center**	CT	6/7/2017	Electronic	Medical/Healthcare	Yes - Published #	**6,000**

On Saturday, April 8, 2017, Southwest's 1046 Fairfield Avenue site was broken into and four desktop computers, one laptop, and other miscellaneous items were stolen. On Friday, April 14, 2017, there was another break in at Southwest's 510 Clinton Avenue site.

Attribution 1 Publication: databreaches.net / hipaajournal.com / N Author:
Article Title: Southwest Community Health Center notifies patients after two burglaries
Article URL: https://www.databreaches.net/southwest-community-health-center-notifies-patients-after-two-burglaries/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170608-02	**Airway Oxygen, Inc. / Purity Cylinder Gases, Inc.**	MI	6/5/2017	Electronic	Medical/Healthcare	Yes - Published #	**497,020**

On the evening of Apri l 18, 2017, we learned that unidentified criminal(s) had gained access to our technical infrastructure and installed ransomware in order to deny Purity Cylinder and Airway Oxygen, two affiliated companies, access to their own data. The types of protected health information that were involved in the breach include some or all of the following data regarding our customer/end users and payment sources: full name, home address, birth date, telephone number, diagnosis, the type of service we are providing you, and health insurance policy numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / MT AG's office / NH AG' Author:
Article Title: Airway Oxygen, Inc. / Purity Cylinder Gases, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Airway%20Oxygen,%20Inc%20SBN%20to%20Consume

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170608-01	**Townsends**	IN	5/30/2017	Electronic	Business	Yes - Unknown #	**Unknown**

The incident appears to have occurred as a result of an unauthorized party gaining access to certain customer data during data transfer to our credit card processor. The incident caused certain secured personal information, including name, address, credit and/or debit card account number, and credit and/or debit card security codes to be potentially exposed to unauthorized individuals.

Attribution 1 Publication: VT AG's office / MD AG's office Author:
Article Title: Townsends
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Jas.%20Townsend%20&%20Son,%20Inc.%20SBN%20t

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170607-02	**Mississippi Division of Medicaid**	MS	5/26/2017	Electronic	Government/Military	Yes - Published #	**5,220**

On April 7, 2017, DOM officials became aware of an issue with the online service the agency used to create forms posted to DOM's website (http://medicaid.ms.gov). Once an online form was submitted the information was also emailed to designated staff within the agency. The email containing the information was not transmitted in a secure manner (i.e. encrypted). This resulted in the possible exposure of information that may have been entered into certain online forms.

Attribution 1 Publication: hhs.gov / databreaches.net / medicaid.m Author:
Article Title: Mississippi Division of Medicaid
Article URL: https://medicaid.ms.gov/dom-informs-individuals-of-possible-exposure-of-protected-health-information/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170607-01	**Northern Humboldt Union High School District**	CA	5/26/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

On an unknown date, a person or persons accessed protected files within the NHUHSD's computer database. A student reported to NHUHSD on April24, 2017 that this information was on a website, and NHCHSD immediately notified school administrators. In this case, the information is considered "personally identifiable" because it included "a user name or email address, in combination with a password or security question and answer that would permit access to an online account." Cal. Civ. Code § 1798.82(h)(2).

Attribution 1 Publication: CA AG's office Author:
Article Title: Northern Humboldt Union High School District
Article URL: https://oag.ca.gov/system/files/Northern%20Humboldt%20notice%20only%20SecurityBreach2017_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170606-06	**optionsXpress, Inc. by Charles Schwab**	IL	5/24/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**940**

On May 4, 2017, we learned that documents containing personal information associated with your optionsXpress account(s) became searchable on line due to links you created to your optionsXpress documents. Based upon our investigation, the information in the documents at issue included name and address, as well as the account number, account balance, and positions for one or more of your accounts. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / CT AG's office / MD AG Author:
Article Title: optionsXpress, Inc. by Charles Schwab
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/optionsxpress-20170524.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170606-05	**ITA Group, Inc.**	IA	5/11/2017	Electronic	Business	Yes - Unknown #	**Unknown**

ITA recently discovered that a system error associated with the incentive program for one of its clients was temporarily allowing for potential unauthorized access to certain program participants' account information.

Attribution 1 Publication: NH AG's office / CT AG's office Author:
Article Title: ITA Group, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/ita-group-20170511.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170606-04	**Clysar, LLC**	IA	5/26/2017	Paper Data	Business	Yes - Unknown #	**Unknown**

On approximately January 23 , 2017, Clysar learned that certain employee W-2 forms may have been potentially compromised when one of its third-party providers transmitted its employees' paper W-2 information through the Postal Service, and the package containing those documents apparently was damaged in a way that could have resulted in the disclosure of some of those forms.

Attribution 1 Publication: NH AG's office Author:
Article Title: Clysar, LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/clysar-20170526.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170606-03	**Louisville Hall of Justice**	KY	6/5/2017	Electronic	Government/Military	Yes - Unknown #	**Unknown**

The computer used by two Assistant County Attorneys was taken from a publicly accessible conference room. Emails of the two attorneys may have been on the hard drive. Those emails could potentially contain names, Social Security numbers, bank account numbers and driver's license numbers.

Attribution 1 Publication: WDRB.com Author:
Article Title: Computer stolen at the Hall of Justice puts some at risk for identity theft
Article URL: http://www.wdrb.com/story/35593341/computer-stolen-at-the-hall-of-justice-puts-some-at-risk-for-identity-theft

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170606-02	**Victory Medical Center**	TX	6/5/2017	Electronic	Medical/Healthcare	Yes - Published #	**2,000**

A data breach at a local clinic caused the information of about 2,000 patients to leak online, the Austin doctor's office announced Monday. Names, dates of birth, addresses, phone numbers, email addresses, medical account numbers, preferred language, race and ethnicity were disclosed, Victory Medical Center said in a news release Monday.

Attribution 1 Publication: statesman.com / databreaches.net / hip Author:
Article Title: DATA BREACH: Austin patient info could have leaked online as early as 2013, local clinic says
Article URL: https://www.statesman.com/news/local/data-breach-austin-patient-info-could-have-leaked-online-early-2013-local-clini

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170606-01	**Township of Springfield**	NJ	6/6/2017	Electronic	Government/Military	Yes - Published #	**40,061**

The forensic IT experts have confirmed that there was unauthorized access to the server between Feb. 22, 2017 and March 9, 2017, when the threat was eliminated. The information may have included your full name, driver's license or state card identification number, birth date, address, and telephone number. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NY AG's office / MD AG Author:
Article Title: Township of Springfield
Article URL: https://dojmt.gov/wp-content/uploads/Township-of-Springfield.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170605-09	**Sound Community Services**	CT	5/26/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,282**

New London, CT-based Sound Community Services Inc., a not-for-profit provider of education, support and assistance for individuals with persistent mental illness and/or substance abuse disorders has discovered an unauthorized individual has gained access to an employee's email account. The email account was discovered to contained the protected health information of 1,278 individuals. (Exposure number per NY AG's office)

Attribution 1 Publication: hhs.gov / hipaajournal.com / NY AG's off Author:
Article Title: Sound Community Services Discovers Email Account Breach
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170605-08	LKM Medical	OK	6/2/2017	Electronic	Medical/Healthcare	Yes - Published #	3,400

Personal information of about 3,400 customers may have been compromised in an internal theft of a Tulsa-based medical supplier database. In a statement on its website, LKM Medical said two employees on Jan. 3 stole a company computer with customer information stored on it. The employees have been fired.

Attribution 1 Publication: databreaches.net / newsok.com Author:
Article Title: Laptop stolen from Tulsa firm contained customers' personal data
Article URL: http://newsok.com/laptop-stolen-from-tulsa-firm-contained-customers-personal-data/article/5551260

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170605-07	Crimson Trace Corporation	OR	6/2/2017	Electronic	Business	Yes - Published #	6,866

An extensive forensic investigation found that an unauthorized individual was able to gain access to our website and may have compromised payment card information as well as some basic contact information of customers who transacted on the site between June 1, 2016 and May 5, 2017. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / VT AG's office / NH AG' Author:
Article Title: Crimson Trace Corporation
Article URL: https://dojmt.gov/wp-content/uploads/Crimson-Trace-Corporation.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170605-06	North Dakota Department of Human Resources	ND	6/3/2017	Paper Data	Government/Military	Yes - Published #	2,452

On May 10, 2017, a citizen called the department to report finding Medicaid claim resolution worksheet documents, dated 2015 and containing protected health information, discarded in a dumpster in Bismarck. The department recovered the Medicaid worksheets that day, launched an investigation, and has found no evidence that any confidential information has been used improperly or further disclosed.

Attribution 1 Publication: databreaches.net / valleynewslive.com / Author:
Article Title: Nearly 2,500 North Dakotans face a privacy breach
Article URL: http://www.valleynewslive.com/content/news/Nearly-2500--425978384.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170605-05	Trojan Battery Sales, LLC	FL	6/1/2017	Electronic	Business	Yes - Published #	132

Our investigation determined that a total of three employee email accounts were subject to unauthorized logins by an unknown source between mid-February and late April of 2017. Our investigation determined that the following types of information may be at risk because they were contained with email messages and/or electronic attachments stored within one or more of the compromised employee email accounts: your name <<clientdef1: Social Security number, driver's license number or state identification card number, credit or debit card information (including card number, expiration date, and card security code)>> (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: Trojan Battery Sales, LLC
Article URL: https://dojmt.gov/wp-content/uploads/Trojan-Battery.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170605-04	Engleberth Construction, Inc.	VT	5/31/2017	Electronic	Business	Yes - Published #	181

On May 18th, an employee of the Company discovered that an unauthorized person, whose IP address appears to be in South Africa, had been using her Company email address. The impacted employee works in human resources. After reviewing her email activity, we determined that she may have been the victim of a "phishing" scam on or about May 3, 2017, in which she provided her email account credentials. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / NY AG' Author:
Article Title: Engleberth Construction, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Engelbeth%20Construction,%20Inc.%20SBN%20to%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170605-03	**Angliss & Colohan, P.C.**	CT	5/30/2017	Electronic	Business	Yes - Published #	**479**

On March 6, 2017, we discovered that Angliss & Colohan, P.C. had become the target of a phishing email campaign and that an employee had clicked on the phishing email and entered their credentials. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / CT AG' Author:
Article Title: Angliss & Colohan, P.C.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Angliss%20&%20Colohan,%20P.C%20SBN%20to%20C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170605-02	**MyFreedomSmokes.com**	NC	6/5/2017	Electronic	Business	Yes - Published #	**21,957**

Although the incident is still under investigation, it appears that between approximately March 7, 2017 and April 25, 2017, an unauthorized individual was able to obtain access to portions of our website and insert
malicious code that was designed to capture payment information provided in connection with a purchase. We believe that the incident could have affected certain information (including name, address, email address, telephone number, payment card account number, expiration date, and card verification value (CVV) of individuals who made a purchase on the website. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MD AG's office / NY AG Author:
Article Title: My Freedom Smokes
Article URL: https://oag.ca.gov/system/files/California%20Notification%20Letter%20%286-5%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170605-01	**Signature Hardware, Inc.**	KY	6/2/2017	Electronic	Business	Yes - Published #	**5,130**

On or around April 24, 2017, an unauthorized person gained access to the third-party platform we utilize to host our checkout process. The information that may have been accessed includes any information entered during the Signature hardware checkout process, including credit card number, expiration date, and CVV number (the three or four digits on the back of your card). (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / OR AG's office / MT AG Author:
Article Title: Signature Hardware, Inc.
Article URL: https://oag.ca.gov/system/files/Consumer%20Notification_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-10	**Seton Healthcare**	TX	5/31/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

Austin-based Seton Healthcare is investigating a potential breach after officials detected 'suspicious activity' on its computer network on Sunday night.

Attribution 1 Publication: healthcareitnews.com Author:
Article Title: Seton Healthcare investigating potential breach after virus attack
Article URL: http://www.healthcareitnews.com/news/seton-healthcare-investigating-potential-breach-after-virus-attack

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-09	**D. Andrew Loomis MD, Paula Schulze MD,Tammara**	WA	5/24/2017	Electronic	Medical/Healthcare	Yes - Published #	**9,000**

D. Andrew Loomis MD, Paula Schulze MD,Tammara Stefanelli MD, Christen Vu DO, Anja Crider MD, Susan Clabots-Sheets ARNP WA Healthcare Provider 9000 05/24/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: D. Andrew Loomis MD, Paula Schulze MD,Tammara Stefanelli MD, Christen Vu DO, Anja Crider MD, Susan Clabots-Sheets A
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=AEBAF2F9B540A3C065F798BA43EAA86C

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-08	Kmart / Sears Holding Company	IL	6/1/2017	Electronic	Business	Yes - Published #	35,155

"Our Kmart store payment data systems were infected with a form of malicious code that was undetectable by current anti-virus systems and application controls," Howard Riefs, a spokesman for Sears Holding, said in a statement. "Once aware of the new malicious code, we quickly removed it and contained the event. We are confident that our customers can safely use their credit and debit cards in our retail stores." (Exposure number per NY AG's office per notification from Discover)

Attribution 1 Publication: patch.com / ME AG's office / NY AG's of Author:
Article Title: Kmart Data Breach: Company Confirms Customer Credit Card Information Stolen
Article URL: https://patch.com/us/across-america/kmart-confirms-credit-card-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-07	Office of Dr. Kadri / Plastic Surgery Clinic	CA	5/31/2017	Paper Data	Medical/Healthcare	Yes - Published #	15,000

A spokesperson for Dr. Kadri says some of his clients are celebrities whose medical records may now be in jeopardy. That's because the records of 15,000 patients were stolen — they say by a disgruntled former staffer fired for allegedly stealing from the practice.

Attribution 1 Publication: hollywoodreporter.com Author:
Article Title: Beverly Hills Plastic Surgery Clinic Rocked by Patient Records Heist: "There Is Still Outstanding Stolen Property"
Article URL: http://www.hollywoodreporter.com/news/beverly-hills-plastic-surgery-identity-theft-is-still-outstanding-stolen-material-

Attribution 2 Publication: losangeles.cbslocal.com Author:
Article Title: Privacy Breach at Beverly Hills Clinic Puts Thousands of Patients, Some Celebrities, at Risk
Article URL: http://losangeles.cbslocal.com/2017/05/31/privacy-breach-beverly-hills-clinic/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-06	OneLogin	CA	6/1/2017	Electronic	Business	Yes - Unknown #	Unknown

OneLogin, an online service that lets users manage logins to sites and apps from a single platform, says it has suffered a security breach in which customer data was compromised, including the ability to decrypt encrypted data.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: OneLogin: Breach Exposed Ability to Decrypt Data
Article URL: https://krebsonsecurity.com/2017/06/onelogin-breach-exposed-ability-to-decrypt-data/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-05	Pinto Mucenski Hooper VanHouse & Co.	NY	5/23/2017	Electronic	Business	Yes - Published #	267

On April 8, 2017, we discovered that your tax information stored within our server may have been accessed by an unknown, unauthorized third-party. The investigation determined that your name, address, Social Security number and other tax information may have been accessed by an unauthorized third party. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / MD AG's office /AG's off Author:
Article Title: Pinto Mucenski Hooper VanHouse & Co.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Pinto,%20Mucenski,%20Hooper,%20VanHouse%20&%

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-04	Stephenville Medical & Surgical Clinic	TX	6/1/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

When an administrator at Stephenville Medical & Surgical Clinic, in Stephenville, Texas, received a request for a blank medical record release form on May 19, the unnamed employee in the Medical Records Department sent instead a spreadsheet containing data on former patients, according to an article in the Stephenville Empire-Tribune.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Data incident at Stephenville Medical & Surgical Clinic in Texas
Article URL: https://www.scmagazine.com/data-incident-at-stephenville-medical-surgical-clinic-in-texas/article/665817/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-03	**Children's Mercy Hospital**	MO	5/31/2017	Electronic	Medical/Healthcare	Yes - Published #	**5,511**

A website created by a physician at Children's Mercy Hospital in Kansas City, MO has recently been discovered to lack appropriate security protections, potentially allowing the protected health information of 5,511 patients to be viewed by unauthorized individuals.

Attribution 1 Publication: hipaajournal.com / MT AG's office Author:
Article Title: Children's Mercy Hospital Discovers Unauthorized Website Exposed 5,500 Patients' PHI
Article URL: http://www.hipaajournal.com/childrens-mercy-hospital-discovers-unauthorized-website-exposed-5500-patients-phi-88

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-02	**Keith M. Southwood, CPA, Inc.**	CA	3/29/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On April 3, 2017, the firm discovered that an unauthorized third party gained access to its secure computer network on or about March 29, 2017. As a result of the incident, your personal information, including name, address, date of birth, social security number, and/or financial account information may have been exposed.

Attribution 1 Publication: CA AG's office Author:
Article Title: Keith M. Southwood, CPA, Inc.
Article URL: https://oag.ca.gov/system/files/Adult%20Notification%20Sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170601-01	**Funding Circle USA, Inc.**	CA	4/27/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**6,000**

On April 27, 2017, a professional security researcher discovered a vulnerability in one of our databases that included some information about our U.S. customers, and notified us shortly after.

Attribution 1 Publication: CA AG's office / Forbes Author:
Article Title: Funding Circle Error Exposes 6,000 SSNs Of American Clients
Article URL: https://www.forbes.com/sites/thomasbrewster/2017/05/10/funding-circle-open-database-exposes-6000-us-clients/ - d2c

Attribution 2 Publication: CA AG's office Author:
Article Title: Funding Circle USA, Inc.
Article URL: https://oag.ca.gov/system/files/CA%20Consumer%20Notification%20%285.25.17%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170531-01	**University of Alaska**	AK	5/31/2017	Electronic	Educational	Yes - Published #	**25,000**

Approximately 25,000 students, staff, and faculty members associated with the University of Alaska were affected following a successful phishing scam and subsequent data breach late last year.

Attribution 1 Publication: ktuu.com / scmagazine.com Author:
Article Title: University of Alaska: thousands affected by data breach, including names, social security numbers
Article URL: http://www.ktuu.com/content/news/University-of-Alaska-thousands-affected-by-data-breach-including-social-security-i

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170530-07	**Cameron County**	TX	5/23/2017	Electronic	Government/Military	Yes - Unknown #	**Unknown**

The personal information of tens of thousands of Rio Grande Valley residents were put at risk, as estimated in a CHANNEL 5 NEWS investigation of a computer server found at a local flea market. Tens of thousands of names, addresses and Social Security numbers were contained on files accessed without the need of a password. The server once belonged to Cameron County.

Attribution 1 Publication: databreaches.net / KRGV.com Author:
Article Title: Investigation: Your Life for Sale
Article URL: http://www.krgv.com/story/35502088/investigation-your-life-for-sale

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170530-06	**Augusta University / Augusta University Medical Center**	GA	5/28/2017	Electronic	Medical/Healthcare	Yes - Published #	**5,600**

Augusta University says a phishing attack hit faculty email accounts containing the health information of patients. In addition to patients' full names, the e-mail accounts may have contained any of the following patient information: home address, date of birth, Social Security number, financial account information, medical record number, insurance information.

Attribution 1 Publication: hhs.gov wfxg.com Author:
Article Title: Augusta University / Augusta University Medical Center
Article URL: http://www.wfxg.com/story/35533360/investigation-into-phishing-attack-at-augusta-university

Attribution 2 Publication: hipaajournal.com Author:
Article Title: 5 Months to Notify Patients of Augusta University Medical Center Phishing Attack
Article URL: https://www.hipaajournal.com/augusta-university-medical-center-phishing-attack-8971/

Attribution 3 Publication: WFXG.com/databreaches.net/NH AG's Author:
Article Title: Investigation into phishing attack at Augusta University
Article URL: http://www.wfxg.com/story/35533360/investigation-into-phishing-attack-at-augusta-university

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170530-05	**Mallard Creek High School / Charlotte-Mecklenburg**	NC	5/29/2017	Paper Data	Educational	Yes - Unknown #	**Unknown**

A Channel 9 viewer said she warned Charlotte-Mecklenburg Schools' officials after finding documents with students' names, addresses and other personal information blowing in the wind.

Attribution 1 Publication: WSOCTV.com / databreaches.net Author:
Article Title: Papers with CMS students' sensitive information found blowing in wind
Article URL: http://www.wsoctv.com/news/local/documents-with-cms-students-senstive-information-found-blowing-in-wind/526986

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170530-04	**Trios Health / Kennewick Health System**	WA	5/30/2017	Electronic	Medical/Healthcare	Yes - Published #	**569**

A Trios Health employee improperly accessed the electronic medical records of about 600 patients over 3 1/2 years, the Kennewick health system announced Tuesday morning. The records may have included information related to Trios Health visits, not including visits to outpatient Trios Medical Group providers, as well as diagnoses, demographic information such as addresses, phone numbers and driver's license numbers, and also social security numbers, Trios officials said in a statement.

Attribution 1 Publication: tri-cityherald.com / WA AG's office / hipa Author:
Article Title: Trios Health fires employee over records breach, hundreds of patients affected
Article URL: http://www.tri-cityherald.com/news/local/article153344574.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170530-03	**Arizona Department of Health Services (ADHS)**	AZ	5/30/2017	Paper Data	Government/Military	Yes - Published #	**2,500**

Data collected as part of a newborn screening program run by the Arizona Department of Health Services (ADHS) has been lost in the mail. The information, which was to be used for billing purposes, contained the personal information, financial data and sensitive health information of approximately 2,500 patients.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Arizona Department of Health Services Notifies 2,500 Patients of Potential Loss of PHI
Article URL: http://www.hipaajournal.com/arizona-department-of-health-services-2500-patients-loss-phi-8824/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170530-02	**Beacon Health System**	IN	5/30/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,239**

A former Beacon Health System employee has been discovered to have accessed the medical records of approximately 1,200 patients without authorization over a period of three years. The types of information in the records included patients' names, ages, room numbers, chief medical complaint and the acuity of their illness. Social Security numbers, health insurance information and financial account information were also potentially viewed by the employee.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Beacon Health Employee Improperly Accessed 1,200 Patient Records Over 3 Year Period
Article URL: http://www.hipaajournal.com/beacon-health-employee-improperly-accessed-1200-patient-records-3-year-period-8825/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170530-01	**FastHealth Corporation - multiple entities**	AL	5/26/2017	Electronic	Medical/Healthcare	Yes - Published #	**18,301**

On December 21, 2016, Fasthealth discovered suspicious code on a server. Upon learning of this, we immediately began an investigation and hired a leading computer security firm to assist. On January 24,
2017, the computer security firm determined that an unauthorized third party altered code on FastHealth's web server that was designed to capture payment card information as it was being entered on Fasti-lealth's online bill-pay platforms from January 14, 2016 to December 20,2016. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NY AG's office / NH AG' Author:
Article Title: FastHealth Corporation
Article URL: https://oag.ca.gov/system/files/Fast%20Health%20notice%20only_0.pdf?

Attribution 2 Publication: tehachapines.com Author:
Article Title: Security breach leads to release of information used to pay TVHD, Adventist Health
Article URL: http://www.tehachapinews.com/news/security-breach-leads-to-release-of-information-used-to-pay/article_875d2a22-42

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170526-07	**Humana**	KY	4/21/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

On March 20, 2017 Humana became aware of a significant increase in the number of secure log in errors that were the result of numerous attempts to log into Humana.com and/or Go365.com from foreign countries. The attackers may have gained access to your information on humana.com and/or go365.com, which includes medical, dental and vision claims, spending account information and biometric screening information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170526-06	**Ricoh USA, INC / Equifax**	PA	5/18/2017	Electronic	Business	Yes - Published #	**114**

On April 20, 2017, Equifax Workforce Solutions ("Equifax"), which provides payroll-related services to Ricoh, informed us that it had been investigating potential unauthorized access to its systems. The investigation determined that an unauthorized individual(s) may have accessed some of our current and former employees' payroll information through Equifax's systems. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: Ricoh USA, INC / Equifax
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/ricoh-usa-20170518.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170526-05	**Ives & Sultan, LLP**	NY	5/8/2017	Electronic	Business	Yes - Published #	**2,518**

In March of 2017, Ives & Sultan LLP were notified that certain client tax returns had been fraudulently filed. They immediately opened an investigation and learned that approximately 3,000 client documents had been accessed by an unauthorized party from the secure database hosted by Smart Vault in November of 2016 by utilizing the log-in credentials of an Ives & Sultan employee. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / CT AG's office / NY AG' Author:
Article Title: Ives & Sultan, LLP
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/ives-sultan-20170508.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170526-04	Citizens Financial Group (5/5/2017)	RI	5/5/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We are writing to inform you that personal information such as your name, address, phone number, account number, social security number and other identifying information may have been subject to unauthorized access in April 2017.

Attribution 1 Publication: NH AG's office Author:
Article Title: Citizens Financial Group
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/citizens-financial-group-20170505.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170526-03	Capital First Trust Company	WI	5/15/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 7, 2017 one of Capital First's trust investment advisors informed Capital First that they had detected suspicious activity related to Capital First 's online accounts. On April 7, 2017, the computer forensic company informed Capital First that an unauthorized user had gained access to two Capital First user accounts, which was limited to these users' email accounts and shared files. From our review, the email accounts or shared files may have contained information related to your accounts with us, such as your name, address, Social Security number, driver's license number, credit card number, or your bank account information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Capital First Trust Company
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/capital-first-trust-20170510.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170526-02	University of Wisconsin Health	WI	5/25/2017	Electronic	Medical/Healthcare	Yes - Published #	2,036

UW Health says that 2,036 patients had information compromised after an employee's email account was used by an unauthorized user. In the review, UW Health found some of the emails compromised contained patient information which may have included patients' names; addresses; dates of birth; dates of service; providers' names; reason for visit; medical history and conditions, medications; diagnostic results and/or social history.

Attribution 1 Publication: databreaches.net / wbay.com / WI AG's Author:
Article Title: UW Health: Information on 2,036 patients compromised after data breach
Article URL: http://www.wbay.com/content/news/UW-Health-information-on-2036-patients-compromised-424454484.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170526-01	MolinaHealthcare.com	CA	5/26/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

A security flaw in MolinaHealthcare.com exposed every other patient's data to anyone logged into the site. It is unclear how many records were exposed, but independent researcher Brian Krebs, who received an anonymous tip, suspects potentially all of the records were exposed including names, addresses and dates of birth, as well as potentially sensitive information that may point to specific diseases, such as medical procedure codes and any prescribed medications, according to a May 25 blog post.

Attribution 1 Publication: scmagazine.com / hipaajournal.com Author:
Article Title: MolinaHealthcare.com patient records left exposed
Article URL: https://www.scmagazine.com/molina-healthcare-patient-records-left-exposed-by-simple-method/article/664713/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170525-09	Niskayuna Central School District	NY	5/24/2017	Electronic	Educational	Yes - Published #	945

The personal information of 945 students, both past, and present, was compromised as a result of a thief stealing the laptop of a Niskayuna school psychologist. It is deemed low risk by the school district, in the sense that it did not compromise social security numbers or other significant personal information. However, names, date of birth and addresses were on the computer for over 600 current students and 300 former students.

Attribution 1 Publication: databreaches.net / news10.com Author:
Article Title: Niskayuna school laptop stolen, 945 students' personal information on device
Article URL: http://news10.com/2017/05/24/niskayuna-school-lap-top-stolen-945-students-personal-information-on-device/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170525-08	City of Stillwater	OK	5/24/2017	Electronic	Government/Military	Yes - Published #	3,000

The City of Stillwater announced Wednesday that the information for about 3,000 people has been compromised after an unauthorized party had access to a city computer. "The hacked computer contained no financial information; however, some personal information, such as names, addresses, driver's license numbers, and in some cases social security numbers were potentially accessed," said Sherry Fletcher, the city's director of marketing and public relations.

Attribution 1 Publication: databreaches.net / kfor.com Author:
Article Title: Personal information exposed for 3,000 people in Stillwater after unauthorized access obtained to city computer
Article URL: http://kfor.com/2017/05/24/personal-information-exposed-for-3000-people-in-stillwater-after-unauthorized-access-obtai

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170525-07	SSM Health / DePaul Hospital St. Louis	MO	5/25/2017	Electronic	Medical/Healthcare	Yes - Published #	836

SSM Health has started notifying patients that some of their protected health information was exposed when a portable device was stolen from DePaul Hospital St Louis in Bridgeton, MO. The device contained the protected health information of 836 patients, including names, medical record numbers, dates of birth and brief details of patients' chief health complaint.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Stolen Electromyography Device Contained 836 Patients PHI, says SSM Health
Article URL: http://www.hipaajournal.com/stolen-electromyography-device-contained-836-patients-phi-says-ssm-health-8822/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170525-05	Frontier Airlines	CO	5/19/2017	Electronic	Business	Yes - Published #	3,605

Based on our review, we have determined that a former employee, prior to being dismissed by the company, may have viewed and disclosed your personal and financial information, including your name, address, date of birth, Social Security number, passport number, and your checking account and bank routing numbers. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170525-04	Bank of the West	CA	5/25/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On April 9, 2017, the Bank's security teams identified instances of unauthorized account withdrawals at the our AIMs in several Southern California cities. We immediately contacted Law enforcement and began taking steps to review our ATM network. Our review found that devices known as "ATM skimming devices" had been installed and removed from seven of our ATMs in Southern California.

Attribution 1 Publication: CA AG's office Author:
Article Title: Bank of the West
Article URL: https://oag.ca.gov/system/files/LS%200517-050%20ATM%20Skimming-GLBA%20Incident_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170525-03	Char-Broil, LLC	GA	3/22/2017	Electronic	Business	Yes - Published #	17,124

On April 21, 2017, we discovered that an unauthorized third party uploaded malicious computer code to the system that hosts Charbroil.com. The information potentially impacted includes information provided when making a payment card purchase on Charbroil.com during the time frame above, including your name, billing address, phone number, payment card number, expiration date, and CVV2 code. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / VT AG's office / MT AG' Author:
Article Title: Char-Broil, LLC
Article URL: https://oag.ca.gov/system/files/R612_v02.pdf_Adult_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170525-02	Allrecipes.com	WA	5/25/2017	Electronic	Business	Yes - Unknown #	Unknown

We recently determined that the email address and password typed into allrecipes.com by members when they created or logged into their accounts prior to June 2013 may have been intercepted by an unauthorized third party.

Attribution 1 Publication: CA AG's office / WI AG's office Author:
Article Title: Allrecipes.com
Article URL: https://oag.ca.gov/system/files/Meredith%20-%20Final%20consumer%20notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170525-01	Punch Bowl	MI	5/24/2017	Electronic	Business	Yes - Published #	2,301

Both former workers and several other employees just received letters from Punch Bowl informing them that the business was a victim of a phishing scheme. W-2 forms including names, addresses and social security numbers of potentially hundreds of employees have been electronically leaked. (Exposure number per NY AG's office)

Attribution 1 Publication: fox2detroit.com / NY AG's office Author:
Article Title: Security Breach at Punch Bowl Social;Employee Personal information compromised
Article URL: http://www.fox2detroit.com/news/local-news/256800320-story

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170524-01	BMO Harris Bank (5/17)	IL	5/24/2017	Electronic	Banking/Credit/Financial	Yes - Published #	38,391

On Monday, May 15, 2017, BMO Harris Bank discovered an error in the production of 2016 IRS Form 5498 for BMO Harris Bank IRA accounts through which some customers received their own Form 5498 along with another customer's Form 5498, while other customers did not receive any form. The compromised information included name, address, the last four digits of the Social Security number, account number, IRA contributions for 2016, and Fair Market Value of the IRA as of December 31, 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: WI AG's office / CA AG's office / MT AG' Author:
Article Title: BMO Harris Bank
Article URL: https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-15	Karas & Bradford	MD	1/3/2017	Electronic	Business	Yes - Unknown #	Unknown

On May 6, 2016, K&B learned that hackers had installed spyware on at least two of K&B's computers, and that the spyware gave the hackers the ability to see, read and copy documents and files on K&B's system, including documents and files which contain certain personally identifiable information of individuals to whom K&B provides services.

Attribution 1 Publication: MD AG's office Author:
Article Title: Karas & Bradford
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-277029.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-14	Crosman Corporation	NY	1/4/2017	Electronic	Business	Yes - Unknown #	Unknown

Crosman Corporation, an entity located in Bloomfield, New York, has experienced an unlawful breach of our systems on or about December 6-8, 2016. The specific types of personal information impacted could include: first and last name; email address and/or username, in combination with the password permitting account to an online Crosman account; and credit card number and security code.

Attribution 1 Publication: MD AG's office / ME AG's office Author:
Article Title: Crosman Corporation
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-277028.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-13	**Alliance Southwest, LLC / Huntington Apartments**	FL	1/9/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Please be advised that on October 13, 2016, our client, Alliance Southwest, LLC, who managed The Huntington Apartments ("Huntington") learned that an inoperable desktop computer which may have contained personal information of some former Huntington tenants was lost by its mail vendor. The personal information likely included former tenants' names, addresses, and Social Security Numbers.

Attribution 1 Publication: MD AG's office / CT AG's office Author:
Article Title: Alliance Southwest, LLC / Huntington Apartments
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-278461.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-12	**Royal Alliance & Associates**	NY	1/11/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

The computer I use for business at our branch office was accessed by an unauthorized individual as part of a phishing incident. Although my computer did contain anti-malware and virus programs, it was determined that the unauthorized individual could have accessed the local computer files. Your personal information, including your name, address and Social Security Number, was available on the computer.

Attribution 1 Publication: MD AG's office Author:
Article Title: Royal Alliance & Associates
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-278460.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-11	**OneMain Financial Group**	MD	1/12/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

Between October 17, 2016 and November 15, 2016, the former employee may have recorded for her own personal use customers' checking account and credit and debit card account information that was provided to her by our customers by phone who were making payments to us or our affiliates by phone.

Attribution 1 Publication: MD AG's office Author:
Article Title: OneMain Financial Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-278455.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-10	**Telecom Insurance Group**	MD	1/12/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We recently became aware of a situation where there was unauthorized access to our employee W2s. The W-2 information includes name, address and social security number information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Telecom Insurance Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-278452.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-09	**Stark Investments**	WI	1/13/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

Stark recently discovered evidence suggesting that from November 20, 2016 through November 22, 2016, an unauthorized person or persons may have gained access to a Stark employee's email account. Stark is in possession of certain subscription documents that contain the name, address, date of birth, social security number, bank wire information, and Stark account numbers of investors.

Attribution 1 Publication: MD AG's office / CT AG's office Author:
Article Title: Stark Investments
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-278451.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-08	MBA Consulting Services	VA	1/23/2017	Electronic	Business	Yes - Published #	360

During this incident, which occurred on January 6, 2017, there was an unauthorized release of 2015 W-2 tax forms for MBA employees and contractors. (Exposure number per NY AG's office)

Attribution 1
Publication: MD AG's office / NY AG's office Author:
Article Title: MBA Consulting Services
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-278695.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-07	Sirius XM	DC	1/24/2017	Electronic	Business	Yes - Unknown #	Unknown

Certain Sirius XM employees became aware that a data security incident occurred on January 6, 2017 that involved a potential intrusion into the credentials of eight (8) Maryland residents into their online accounts at Sirius XM (the "OAC"). The customers' Sirius XM customer account number, street address, email address, nickname ofthe customers' radio (i.e., an automobile radio) and the customers' method of payment for the Sirius XM services (i.e., credit card or check) may have been accessed.

Attribution 1
Publication: MD AG's office Author:
Article Title: Sirius XM
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-278712.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-06	Trinity Private Equity Group	TX	2/1/2017	Electronic	Banking/Credit/Financial	Yes - Published #	138

The burglar stole two password-protected laptop computers, one of which contained confidential information. The information was not encrypted and included the names, social security numbers, and addresses of customers, including ourselves and our families, who received an IRS Form 1099 from TPEG or investor entities affiliated with TPEG for the years 2014 and 2015. (Exposure number per NY AG's office)

Attribution 1
Publication: MD AG's office / NY AG's office Author:
Article Title: Trinity Private Equity Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280135.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-05	Roundpoint Mortgage Servicing Corporation	NC	2/2/2017	Electronic	Business	Yes - Unknown #	Unknown

One of RoundPoint's print vendors had a manual error by one of their employees. The vendor's employee disregarded our vendor's policy and quality control process which resulted in four (4) Maryland resident's personal information being sent to a third party.

Attribution 1
Publication: MD AG's office Author:
Article Title: Roundpoint Mortgage Servicing Corporation
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280139.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-04	Goldberg, Miller and Rubin	PA	2/23/2017	Electronic	Business	Yes - Published #	5,700

GMR was notified in late October of 2016 by a security researcher that he had been able to access electronic files relating to some of GMR's cases. The electronic files were stored at a facility in Philadelphia, PA maintained by GMR's third-party service provider for backup and disaster recovery purposes. (Exposure number per NY AG's office)

Attribution 1
Publication: MD AG's office / NY AG's office Author:
Article Title: Goldberg, Miller and Rubin
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280142%20(update).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-03	**Blue Cross Blue Shield of Kansas City**	MO	5/5/2017	Electronic	Medical/Healthcare	Yes - Published #	**725**

Blue Cross and Blue Shield of Kansas City MO Health Plan 725 05/05/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Blue Cross Blue Shield of Kansas City
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=5DCE7D73969FAD091F6C0973BCBFDA45

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-02	**KURU Fotowear**	UT	3/3/2017	Electronic	Business	Yes - Published #	**18,138**

We recently learned that we were the victims of a sophisticated cyber-attack that may affect the security of your payment information. Through the ongoing third-party forensic investigations, we confirmed on February 23, 2017 that malware may have stolen credit or debit card data from some credit and debit cards used at www.kurufootwear.com between December 20, 2016 and March 3, 2017. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / WI AG's office / NH AG' Author:
Article Title: KURU Fotowear
Article URL: https://oag.ca.gov/system/files/Kuru%20-Notice%20ONLY-%20CA%20Exhibit%201_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170523-01	**Florida Department of Agriculture and Consumer**	FL	5/23/2017	Electronic	Government/Military	Yes - Published #	**470**

A data breach at the Florida's Department of Agriculture and Consumer Services (FDACS) has put the personal information of thousands of people at risk, according to the Tampa Bay Times. Social Security numbers of as many as 469 people were exposed, as well as personal data on more than 16,000 holders of concealed weapon permits.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Breach of Florida agency exposes SSNs and concealed weapons license holders
Article URL: https://www.scmagazine.com/breach-of-florida-agency-exposes-ssns-and-concealed-weapons-license-holders/article/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170522-03	**AT&T**	TX	5/19/2017	Electronic	Business	Yes - Published #	**14,878**

Our monitoring shows that an unauthorized person may have acquired your att.com ID and password and used these credentials to access your online account. The potential unauthorized account access may have included a single page on which your driver's license number was visible. Your mobile service and device were not affected. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / VT AG's office / NH AG' Author:
Article Title: AT&T
Article URL: https://dojmt.gov/wp-content/uploads/ATT.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170522-02	**Michael T. Blevins, Inc.**	CA	5/19/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Based on their investigation, it appears that an unauthorized individual was able to gain access to our computer network for limited periods of time over the course of several days in late March and, while there, may have been able to access certain client files stored in our systems.

Attribution 1 Publication: CA AG's office / NH AG's office / CT AG' Author:
Article Title: Michael T. Blevins, Inc.
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_10.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170522-01	**Mt. Diablo Unifed School District**	CA	4/27/2017	Electronic	Educational	Yes - Published #	**600**

On April 27, 2017, when parents tried to access their student's data through the HomeLink Portal, they were able to view information, as described below, of a student other than their own. The period of time parents and students had inadvertent exposure to another student's information was one hour—between 8:00 p.m. and 9:00 p.m. and the data of approximately 600 families was exposed.

Attribution 1 Publication: CA AG's office Author:
Article Title: Mt. Diablo Unifed School District
Article URL: https://oag.ca.gov/system/files/Revised%20Data%20Breach%20Letter%205-12-17_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170519-06	**Citibank, NA**	SD	2/2/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

On approximately November 25, 2016, we learned that an employee of a contractor used by Citibank to process credit card applications attempted to take information reflected on your application from the processing center. The information included your name, address, telephone number, Social Security and/or passport number, and date of birth.

Attribution 1 Publication: MD AG's office Author:
Article Title: Citibank, NA
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280544.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170519-05	**Canal Insurance Company**	SC	2/8/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On or around September 12, 20 16, Canal detected unauthorized access to one of its employee's email accounts as a result of a complex phishing incident. Based on its investigation, Canal has determined that the compromised account contained the residents' full names and either one or more of the following: dates of birth, driver's license numbers, Social Security numbers and certain protected health information in relation to a worker's compensation claim.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Canal Insurance Company
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280617.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170519-04	**Stroh, Johnson & Company LLP**	OH	2/14/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On February 7, 2017, we obtained confirmation that an unauthorized third party had infiltrated our system and accessed client information, including tax files for 2015. The information accessed included client names, addresses, dates of birth, Social Security numbers, and bank account numbers.

Attribution 1 Publication: MD AG's office Author:
Article Title: Stroh, Johnson & Company LLP
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280611.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170519-03	**Viacom, Inc.**	NY	2/28/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Sometime over the weekend of February 3 – February 6, 2017, computer equipment was stolen from a Viacom Inc. office in California. Personal information potentially contained on the stolen equipment may include: name, address, telephone number, email address, birth date, Social Security number, and/or drivers' license number.

Attribution 1 Publication: MD AG's office / ME AG's office / NY AG Author:
Article Title: Viacom, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280215.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170519-02	**Barton Oaks Dental Group (Neeley-Nemeth, LLP)**	TX	5/18/2017	Electronic	Medical/Healthcare	Yes - Published #	**17,090**

On March 23, 2017, Barton Oaks incurred a ransomware attack in which certain of our servers, and PCs were encrypted. Because we take the security of all patients and their information very seriously, we have decided to treat this incident as one that may have resulted in the disclosure of your medical and personal information (which includes your name, address, date of birth, Social Security number, and medical information).

Attribution 1 Publication: VT AG's office / MT AG's office / NY AG' Author:
Article Title: Barton Oaks Dental Group (Neeley-Nemeth, LLP)
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Barton%20Oaks%20Dental%20Group%20SBN%20to%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170519-01	**HSX.com**	CA	5/19/2017	Electronic	Business	Yes - Unknown #	**Unknown**

HSX.com became aware on May 4th that your personal information may have been accessed without authorization. We are committed to protecting your personal information, and immediately acted as noted below.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170518-05	**DRB Systems, LLC / Multiple Car Washes Nationwide**	OH	5/9/2017	Electronic	Business	Yes - Unknown #	**Unknown**

DRB Systems advised the company that the intruder placed malware on their point-of-sale system, and by doing so gained access to customers' payment card data, including the cardholder's first and last name, payment card number, and security code. (car washes)

Attribution 1 Publication: seviernewsmessenger.com Author:
Article Title: Hackers Gain Access to Vol Magic Wash Customer Payment Information
Article URL: http://www.seviernewsmessenger.com/2017/05/09/vol-magic-wash-data-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170518-04	**San Jose City College / Evergreen Valley**	CA	5/16/2017	Electronic	Educational	Yes - Published #	**1,150**

A data breach running since spring 2014 on the district security system was discovered in November. The names, date of birth and social security numbers of about 1,000 of spring 2013 students and about 150 employees in San Jose City and Evergreen colleges had been accessible on the district website for more than two years, public information officer at the Chancellor's office Ryan Brown said.

Attribution 1 Publication: sjcctimes.com Author:
Article Title: 1,000 SJCC and Evergreen Valley students at risk
Article URL: http://sjcctimes.com/11442/news/1000-sjcc-evergreen-valley-students-risk/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170518-03	**Jones Family Practice, PA**	NC	5/5/2017	Electronic	Medical/Healthcare	Yes - Published #	**742**

Jones Family Practice, P.A. NC Healthcare Provider 742 05/05/2017 Unauthorized Access/Disclosure Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Jones Family Practice, PA
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=2341D67CD6DD6A258609927600EE9B12

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170518-02	**Edmodo**	CA	5/11/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Hacker Steals Millions of User Account Details from Education Platform Edmodo. The data includes usernames, email addresses, and hashed passwords.

Attribution 1 Publication: motherboard.vice.com Author:
Article Title: Hacker Steals Millions of User Account Details from Education Platform Edmodo
Article URL: https://motherboard.vice.com/en_us/article/hacker-steals-millions-of-user-account-details-from-education-platform-ed

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170518-01	Rite Aid Online Store	PA	4/11/2017	Electronic	Business	Yes - Published #	18,680

We recently learned that unauthorized third parties accessed Rite Aid Online Store's e-commerce platform and acquired certain personal information of customers who manually entered their payment card details at the online store between January 30, 2017 and April 11, 2017. The personal information that may have been affected includes your name, address, email address, and payment card data, including credit card number, expiration date, and card verification number. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / OR AG's office / hipaajo Author:
Article Title: Rite Aid Online Store
Article URL: https://oag.ca.gov/system/files/Rite%20Aid%20Online%20Store%2C%20Inc.%20Individual%20Notification%20Letter_6

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-16	Jolicoeur & Associates	CA	2/17/2017	Electronic	Business	Yes - Unknown #	Unknown

The forensic investigation is now completed and the unauthorized access was determined to be limited to my email account. Given the nature of our relationship, this information may have included copies of your tax returns, brokerage statements, credit card statements, and bank statements which could include your: name, gender, birth date, telephone number(s), address, social security number, all employment (W-2) information, 1099 information, direct deposit bank account information, including account number and routing information (if provided to me), and supporting records.

Attribution 1 Publication: MD AG's office Author:
Article Title: Jolicoeur & Associates
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280183.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-15	Zelnick, Mann and Winikur, PC	PA	2/21/2017	Electronic	Business	Yes - Published #	1,190

On January 15, 2017, Zelnick, Mann and Winikur, PC ("Ze lnick") determined that a number of our former employees who recently left the firm to start their own business took some of Zelnick's client's records
with them without Zelnick's a uthoriza tion. These records contain the names, addresses, social security numbers, and financial information belonging to some of our clients. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Zelnick, Mann and Winikur, PC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280189.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-14	State Bank of Lincoln	IL	2/21/2017	Electronic	Banking/Credit/Financial	Yes - Published #	5,598

On January 4, 2017, State Bank of Lincoln determined an employee's email account, which was password-protected, was accessed by an unauthorized individual. While the investigation is ongoing, State Bank of Lincoln determined on February 4, 2017 that the names and a combination of one or more of the following types of information about
certain Maryland residents was contained in the email account at the time of the unauthorized access: Social Security number, driver's license number, financial account number, or credit card information. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / ME AG's office / NY AG Author:
Article Title: State Bank of Lincoln
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280194.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-13	**Ralph A. Strafaci**	NJ	2/22/2017	Electronic	Business	Yes - Published #	**159**

On December 22, 2016, I discovered that the credentials to my outside hosted email account were temporarily compromised on that same date. The information related to you and found within the email account is your name, bank account information and] Social Security number. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Ralph A. Strafaci
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280198.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-12	**SunTrust Bank**	GA	2/21/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

SunTrust was notified by a federal law enforcement agency that sensitive personal information regarding customers of multiple organizations including Sun Trust was discovered on the Internet. This law enforcement investigation was unrelated to SunTrust and/or its operations. The information discovered included names, addresses, telephone numbers, email addresses, online banking user IDs and passwords, account number(s), or balances.

Attribution 1 Publication: MD AG's office / ME AG's office Author:
Article Title: SunTrust Bank
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280629.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-11	**EBARA International Corporation**	NV	2/27/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On Thanksgiving Day, November 24, 2016, a customer of EBARA received an email from a legitimate EBARA email account relating to the transfer of funds for payment of services. After a thorough third-party forensics investigation, including an exhausting review of all 42,000 emails within the compromised account, we have determined that your
name and social security number were located within the compromised email account.

Attribution 1 Publication: MD AG's office Author:
Article Title: EBARA International Corporation
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280209.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-10	**Hertzbach & Company, PA**	MD	2/27/2017	Electronic	Business	Yes - Published #	**1,917**

On January 30, 2017, we learned that one of our employees responded to a phishing email designed to appear as if it was a request from Microsoft. The email asked the employee to use his Hertzbach email account user name and password to sign-on to a website that appeared to be an Office 365 portal. (Exposure number per NY AG's office

Attribution 1 Publication: MD AG's office / ME AG's office / NY AG Author:
Article Title: Hertzbach & Company, PA
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280207.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-09	**Erickson Living / TALX**	MD	5/15/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We recently discovered that a user reset PINs to access the accounts of a small number of employees. It appears that the PIN resets and account access were unauthorized. Upon learning of the unauthorized access, TALX promptly took steps to understand what happened, and determined that the unauthori zed user was able to reset the PINs and successfully answer personal questions about the affected individuals.

Attribution 1 Publication: NH AG's office Author:
Article Title: Erickson Living / TALX
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/talx-20170515.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-08	Comcast Biz Leads / ITA Group	PA	5/11/2017	Electronic	Business	Yes - Unknown #	Unknown

It was discovered on April 7, 2017 that a system error associated with the website was temporarily allowing for potential unauthorized access to certain program participants' account information. The sensitive information in your account that was accessible included the bank account information associated with the referral program.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-07	Fidelity National Financial, Inc. / Ceridian Corporation	FL	5/4/2017	Electronic	Banking/Credit/Financial	Yes - Published #	236

Based on that review, we have reason to believe that the fraudster created several online accounts with the tax service vendor between January 11, 2017, and February 23, 2017. Our investigation indicates that one of these online accounts may have provided the fraudster with access to your W-2.Ceridian has advised FNF that the fraudster used legitimate personal information to create the unauthorized accounts to the Ceridian portal and that such information would have included the employee's name, zip code, and Social Security Number. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Fidelity National Financial, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/fidelity-national-financial-20170504.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-06	AeroCare Holdings	FL	5/4/2017	Electronic	Medical/Healthcare	Yes - Published #	860

AeroCare Holdings FL Healthcare Provider 860 05/04/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: AeroCare Holdings
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=FDCE1A3828FDD71804D8D11F8A2E3101

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-05	Massood & Company, PA	NJ	5/12/2017	Electronic	Business	Yes - Published #	2,709

On March 28, 2017, Massood & Company, PA ("Massood") received reports of issues with certain client's 2016 tax filings. Massood immediately launched an investigation and determined, through this investigation, that it was the target of a data security incident that affected the security of some personal information for certain clients. The information relating to you that was present on the affected systems may include the following categories of information: (1) name; (2) address; (3) Social Security number; (4) wage/salary information; and (5) date of birth. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / MD AG's office / NY AG' Author:
Article Title: Massood & Company, PA
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Massood%20&%20Company,%20PA%20SBN%20to%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-04	Rutland Regional Medical Center	VT	5/16/2017	Electronic	Medical/Healthcare	Yes - Published #	665

Rutland Regional Medical Center is facing privacy questions after sending out a patient survey that revealed more than 700 email addresses.

Attribution 1 Publication: databreaches.net / hipaajournal.com Author:
Article Title: Email gaffe exposes more than 700 Rutland Regional Medical Center patient email addresses in survey request
Article URL: http://www.burlingtonfreepress.com/story/news/local/vermont/2017/05/15/rutland-regional-medical-center-reveals-pati

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-03	DocuSign	CA	5/17/2017	Electronic	Business	Yes - Unknown #	Unknown

DocuSign announced that a malicious third party had accessed "a separate, non-core system that allows us to communicate service-related announcements to users via email." "A complete forensic analysis has confirmed that only email addresses were accessed; no names, physical addresses, passwords, Social Security numbers, credit card data or other information was accessed," the company added.

Attribution 1 Publication: krebsonsecurity.com / NY AG's office Author:
Article Title: Breach at DocuSign Led to Targeted Email Malware Campaign
Article URL: https://krebsonsecurity.com/2017/05/breach-at-docusign-led-to-targeted-email-malware-campaign/

Attribution 2 Publication: Docusign.com / esecurityplanet.com Author:
Article Title: DocuSign, Bell Canada Hacked
Article URL: https://trust.docusign.com/en-us/personal-safeguards/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-02	Equitable Tax Service	CA	3/16/2017	Electronic	Business	Yes - Unknown #	Unknown

On the evening of March 16, 2017, Jill Dykes, the owner of ETS, experienced issues logging into her Comcast email account, which she used for professional services on behalf of ETS. This password change occurred without Ms. Dykes' knowledge or consent, indicating potential unauthorized access to her email account and a potential unauthorized disclosure of the data contained in that email account.

Attribution 1 Publication: CA AG's office Author:
Article Title: Equitable Tax Service
Article URL: https://oag.ca.gov/system/files/Sample%20Notice%20Letter_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170517-01	Nicopure Labs, LLC	FL	5/16/2017	Electronic	Business	Yes - Unknown #	Unknown

We have received reports from several customers of fraudulent charges appearing on their payment cards shortly after they were used to make a purchase on our website. During this incident, information entered during the checkout process may or may not have been accessed. This information could have included order ID, name, address, email address, phone number, payment card number, expiration date, and card security code.

Attribution 1 Publication: CA AG's office / OR AG's office / VT AG' Author:
Article Title: Nicopure Labs, LLC
Article URL: https://oag.ca.gov/system/files/NicoPure%20%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170516-01	Tatcha.com	CA	5/5/2017	Electronic	Business	Yes - Unknown #	Unknown

During the early part of 2017, an unauthorized person may have gained access to information keyed into the Tatcha checkout process. While Tatcha does not store credit card information on its systems, the intruder was potentially able to capture information as it was entered. The potentially-affected information includes any information entered during the Tatcha checkout process, including credit card number and expiration date (and card verification value, the three-digit code on the
back of your card), email address, and Tatcha.com account password, as well as your name and mailing and billing addresses.

Attribution 1 Publication: CA AG's office / OR AG's office / VT AG' Author:
Article Title: Tatcha.com
Article URL: https://oag.ca.gov/system/files/ACID_PRINTERPROOFS_20170502_tatcha501_1_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-13	Ameriprise Financial Services, Inc. (2/27)	MN	2/27/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On December 14, 2016, an Ameriprise franchisee advisor contacted a software support company to assist with an issue they were having with software they recently purchased and allowed a third party to connect to their computer to fix the issue. The connection allowed access to the files on their computer.

Attribution 1 Publication: MD AG's office Author:
Article Title: Ameriprise Financial Services, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280206.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-12	**Denison University**	OH	2/27/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

In December 2016, Denison relocated several offices on campus. During the course of this complex move, one desktop computer was misplaced. Denison can confirm that the computer contained the resident's name and address, and may have included Social Security number, date of birth, driver's license number, and passport or employment authorization number. Because the information at issue was related to financial aid, it is possible that the documents submitted may have contained personal information related to students, parents or guardians, and dependents of parents or guardians.

Attribution 1 Publication: MD AG's office Author:
Article Title: Denison University
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280764.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-11	**University of New Mexico Foundation**	NM	5/11/2017	Electronic	Business	Yes - Published #	**23,000**

The University of New Mexico Foundation says a computer server breach may have compromised the financial and other personal information of approximately 22,000 donors. In addition, the Social Security numbers, birth dates and banking information for more than 750 employees, vendors and others may have been illegitimately accessed. (Exposure number per NY AG's office)

Attribution 1 Publication: abqjournal.com / CA AG's office / MD A Author:
Article Title: UNM Foundation server breach includes donors
Article URL: https://www.abqjournal.com/1002352/unm-foundation-server-breached-donor-info-exposed.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-10	**Paratransit Services**	WA	5/12/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Paratransit Services, which provides non-emergency medical and public transportation services in Washington, Oregon and California, fell for an email phishing scam in early March and released all current and former 2016 Paratransit employees' W-2 forms to an unknown party.

Attribution 1 Publication: tdn.com/news Author:
Article Title: Oregon, California falls for email scam, releases employees' W-2s
Article URL: http://tdn.com/news/local/transportation-company-in-washington-oregon-california-falls-for-email-scam/article_5b982

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-09	**Walnut Place**	TX	5/12/2017	Electronic	Business	Yes - Published #	**5,000**

On March 13, 2017, LCS-WP LLC d/b/a Walnut Place ("Walnut Place") leadership discovered that some of its systems had been infected with ransomware (a type of computer malware that encrypts files). The systems that were impacted by this incident contained information including names, Social Security numbers, driver's license numbers, dates of birth, address information, telephone numbers, medical record numbers, health insurance information, payment information (such as banking and credit card information), and clinical/diagnostic information related to Walnut Place patients and residents.

Attribution 1 Publication: databreaches.net / hhs.gov / MD AG's of Author:
Article Title: Walnut Place notifies patients of ransomware attack
Article URL: https://www.databreaches.net/walnut-place-notifies-patients-of-ransomware-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-08	**Office of Robert F. Himmelman**	NY	5/15/2017	Electronic	Business	Yes - Unknown #	**Unknown**

A court-appointed lawyer left documents containing the names and addresses of child-abuse victims — and even explicit details about their cases — to be scattered along a busy Midtown street. Himmelman told
Himmelman told the Post that he put the documents in large plastic bags and left them on the 23rd floor of his Madison Avenue office to be recycled. The files included copies of birth certificates, Social Security numbers and details involving alleged abuse cases with the Administration for Children's Services.

Attribution 1 Publication: nypost.com Author:
Article Title: Attorney's confidential files on abused children scattered on street
Article URL: http://nypost.com/2017/05/15/attorneys-confidential-files-on-abused-children-scattered-on-street/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-07	**Indigo Wild**	MO	5/12/2017	Electronic	Business	Yes - Published #	**1,631**

On April 17, 2017, we discovered that malicious code inserted into our website by sophisticated cybercriminals may have stolen copies of personal information submitted to our website at the time of purchase. (Exposure number per NY AG's office / notification from Discover)

Attribution 1 Publication: OR AG's office / CA AG's office / WA A Author:
Article Title: Indigo Wild
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/821889393

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-06	**PolkBeder**	OH	5/11/2017	Electronic	Business	Yes - Published #	**1,230**

On March 28, 2017, the computer forensics firm notified us that although it found evidence of the system being accessed from the outside, it has not been able to confirm that any PolkBeder client information was removed from our network. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / CT AG's office / NY AG' Author:
Article Title: PolkBeder
Article URL: https://dojmt.gov/wp-content/uploads/PolkBeder.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-05	**Bechtel Oil, Gas & Chemicals Construction Services**	TX	4/27/2017	Electronic	Business	Yes - Published #	**8,937**

On Apri127, 2017, Bechtel Oil, Gas & Chemicals Construction Services, Inc. ("Bechtel") discovered a data incident which may have resulted in unauthorized access or acquisition of your personal information as the result of an inadvertent email sent to other Bechtel email addresses. The incident occurred on April 27, 2017. The data elements involved may have included name, addresses, telephone number, Social Security number, and date of birth. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: Bechtel Oil, Gas & Chemicals
Article URL: https://dojmt.gov/wp-content/uploads/Bechtel-Oil-Gas-Chemicals-Construction.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-04	**Michigan Facial Aesthetic Surgeons dba University**	MI	4/28/2017	Electronic	Medical/Healthcare	Yes - Published #	**3,467**

Michigan Facial Aesthetic Surgeons d/b/a University Physician Group MI Healthcare Provider 3467 04/28/2017 Theft Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Michigan Facial Aesthetic Surgeons dba University Physician 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
ITRC20170515-03	**Clinton County Board of Developmental Disabilities**	OH	5/5/2017	Electronic	Government/Military	Yes - Published #	**1,243**

Clinton County Board of Developmental Disabilities OH Healthcare Provider 1243 05/05/2017 Hacking/IT Incident Network Server

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-02	**D'Angelo & Associates**	CA	5/12/2017	Electronic	Business	Yes - Published #	**2,198**

On Tuesday, April 4, 2017, we encountered suspicious electronic activity in our tax program. On April 24, 2017, the specialized forensic IT firm determined that there was unauthorized access to our system from a foreign IP address on or before March 25, 2017 through April 15, 2017. If you are an individual, this information may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), and direct deposit bank account information (including account number and routing information if provided to us). (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NY AG's office Author:
Article Title: D'Angelo & Associates
Article URL: https://oag.ca.gov/system/files/D%27Angelo%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170515-01	**Brooks Brothers**	NY	3/1/2017	Electronic	Business	Yes - Published #	**25,733**

Brooks Brothers was recently alerted to a potential security incident. Based upon an extensive forensic investigation, it appears that an unauthorized individual was able to gain access to and install malicious software designed to capture payment card information on some of our payment processing systems at our retail and outlet locations. (Exposure number per NY AG's office per notification from Discover)

Attribution 1 Publication: CA AG's office / WA AG's office / NY A Author:
Article Title: Brooks Brothers
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_9.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-27	**National Older Worker Career Center**	CO	2/6/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On January 23, 2017, National Older Worker Career Center ("NOWCC") learned that it was the victim of an email phishing scam. As a result of this scam, an unknown individual fraudulently obtained copies of a small number of certain NOWCC's employees' and former employees' 2015 and 2016 Form W-2's.

Attribution 1 Publication: MD AG's office Author:
Article Title: National Older Worker Career Center
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280148.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-26	**B.C. Ziegler and Company**	IL	2/28/2017	Electronic	Business	Yes - Published #	**145**

On Thursday, February 23,2017, Ziegler was the targeted victim of an e-mail phishing scam. The information that was disclosed was a file containing your 2016 Form W-2, which included your name, address, social security nnmber, wage and associated information from calendar year 2016, and information related to Ziegler. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: B.C. Ziegler and Company
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280546.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-25	Intact Technology, Inc.	MD	2/3/2017	Electronic	Business	Yes - Unknown #	Unknown

On January 19, 2017, a file containing 2016 W-2 data for current and former employees was released to someone fraudulently posing as Intact's CEO, in response to what was perceived to be a legitimate request.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Intact Technology, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280613.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-24	C.A. Short Company	NC	2/22/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 14, 2017, it was brought to C.A. Short's attention that an unauthorized third party unlawfully obtained an electronic file containing certain employee personal information through a criminal scheme known as "phishing" on January 17, 2017. The file contained 2016 Form W-2s of certain current and former employees.

Attribution 1 Publication: MD AG's office Author:
Article Title: C.A. Short Company
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280623.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-23	Calmark Group	IL	2/9/2017	Electronic	Business	Yes - Unknown #	Unknown

Calmark discovered on January 28, 2017, that certain 2015 IRS Form W-2, Wage and Tax Statements of Calmark employees had been stolen as a result of an email phishing scam.

Attribution 1 Publication: MD AG's office Author:
Article Title: Calmark Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280154.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-22	TransCen, Inc.	MD	2/28/2017	Electronic	Business	Yes - Unknown #	Unknown

We recently discovered that our company was the victim of an email spoofing attack on February 3, 2017, by an individual pretending to be our President. A request was made from what appeared to be a legitimate TransCen email address for all 2016 TransCen employee W -2 information.

Attribution 1 Publication: MD AG's office Author:
Article Title: TransCen, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280216.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-21	Colony American Finance, LLC	CA	2/10/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On February 9, 2017, Colony American Finance, LLC (“CAF” or the “Company”) determined that earlier that day, a criminal impersonating a senior Company official received Internal Revenue Service (IRS) W-2 forms for the year 2016, containing the personal information of a number of employees of the Company, including their Social Security numbers.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Colony American Finance, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280165.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-20	San Diego Christian College	CA	2/13/2017	Electronic	Educational	Yes - Unknown #	Unknown

A data breach occurred at San Diego Christian College at approximately 11:00 a.m. on February 6, 2017 after an individual fraudulently acting as the college President requested the 2016 W-2 forms of current and former employees, and the W -2 forms were sent to that individual.

Attribution 1 Publication: MD AG's office Author:
Article Title: San Diego Christian College
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280621.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-19	E.T. Rockville, LLC	MD	2/10/2017	Electronic	Business	Yes - Published #	360

Specifically, on February 3, 2017, an E.T. representative received an email purportedly from its owner and CEO, Mr. Richard Hood, requesting the W-2 forms be sent to him. The E.T. representative complied with the request and sent copies of the W-2s of the employees from its Ellwood Thompson's store in Richmond, VA and its Dawson's Market store in Rockville, MD.

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: E.T. Rockville, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280166.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-18	Medical Depot, Inc.	NY	2/15/2017	Electronic	Business	Yes - Published #	1,023

On Thursday, February 2, 2017, a criminal posing as a member of Drive Medical's management team obtained copies of Drive Medical's employees' Form W-2 for 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Medical Depot, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280176.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-17	Columbia Association	MD	2/16/2017	Electronic	Business	Yes - Unknown #	Unknown

On February13, 2017, Columbia Association was the target of an email phishing scam that resulted in the unauthorized disclosure of our 2016 employees' private information. Specifically, the names, social security numbers and compensation amounts were compromised for present and former employees who received compensation from Columbia Association during 2016.

Attribution 1 Publication: MD AG's office Author:
Article Title: Columbia Association
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280179%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-16	Peak Alarm Company	UT	2/15/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 10, 2017, an unauthorized individual impersonating a Peak Alarm executive contacted a Peak Alarm employee requesting certain information for Peak Alarm personnel. Before it was determined that the request was fraudulent, the Peak Alarm employee provided a file that contained personal information about some of our employees.

Attribution 1 Publication: MD AG's office Author:
Article Title: Peak Alarm Company
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280610.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-15	MGH, Inc.	MD	2/3/2017	Electronic	Business	Yes - Unknown #	Unknown

On January 27, 2017, MGH, Inc. discovered that it had been the victim of an email spoofing scam that resulted in a compromise of the security of employee 2016 IRS Tax Form W-2 information including employee names, addresses, Social Security numbers, and wage information.

Attribution 1 Publication: MD AG's office Author:
Article Title: MGH, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280616.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-14	Biothera Pharmaceuticals, Inc.	MN	2/21/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 10, 2017, a third party fraudulently obtained employee W2 forms from Biothera Pharmaceuticals, Inc. ("Biothera") a client of Dorsey & Whitney LLP. The fraud was perpetrated through an email that was disguised to appear as if it was from an internal employee.

Attribution 1 Publication: MD AG's office Author:
Article Title: Biothera Pharmaceuticals, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280191.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-13	Teletrac, Inc. / Navman Wireless North American	IL	2/9/2017	Electronic	Business	Yes - Published #	465

On February 1, 2017, Teletrac Navman learned that, as the apparent result of a fraudulent email from someone impersonating a senior executive of the company, an employee was tricked into emailing certain
sensitive files to an unknown unauthorized individual. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / CT AG's office / NY AG' Author:
Article Title: Teletrac, Inc. / Navman Wireless North American Limited
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280615.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-12	Jenner & Block	IL	2/9/2017	Electronic	Business	Yes - Published #	859

Jenner & Block LLP has become the victim of an email phishing incident that resulted in disclosure of the information on its current and former employees' 2016 IRS W-2 forms. This incident affects only current and former employees who received a Form W-2 from Jenner & Block for 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Jenner & Block
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280157%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-11	CapTech Ventures	VA	2/17/2017	Electronic	Business	Yes - Published #	785

On February 13, 2017, due to a fraudulent communication to us by someone posing as our Chairman (often referred to as a “phishing” or “spoofing” incident), your 2016 federal W-2 form was sent to an unknown third party. The W-2 form included information relating to your employment, including your name, address, social security number and 2016 wages and tax withholding information. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: CapTech
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280185%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-10	**Grove, Inc.**	IL	2/21/2017	Electronic	Business	Yes - Published #	**1,179**

We believe that employees' W2 information for the year 2016 was inadvertently sent to an improper email address. The information involved may include your name, address, Social Security number, salary, and tax withholding information for 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Grove, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280192.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-09	**Capital One**	VA	5/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

A former employee, while still employed at Capital One®, improperly accessed your Credit Card account to make unauthorized transactions between September and December 2016. Please keep an eye out for other unauthorized transactions (including outside of Capital One) because the former employee saw your account information, such as your name, address, phone number, date of birth, CVV information, transaction history and Social Security number.

Attribution 1 Publication: MT AG's office Author:
Article Title: Capital One
Article URL: https://dojmt.gov/wp-content/uploads/Capital-One-4.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-08	**Wesleyan College**	GA	5/3/2017	Electronic	Educational	Yes - Published #	**3,710**

On April 10, 2017, we learned that an unauthorized individual may have gained access to an employee's email account. We conducted a thorough review of the employee's email account and determined that it may have contained some personal information, including your name, date of birth, Wesleyan ID number, and Social Security number. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / ME AG's office / NY AG Author:
Article Title: Wesleyan College
Article URL: https://dojmt.gov/wp-content/uploads/Wesleyan-College.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-07	**Shock Doctor**	CA	4/28/2017	Electronic	Business	Yes - Published #	**2,420**

On April 6, 20 17, Shock Doctor discovered that your personal information may have been affected when an external actor or actors placed hidden code on the Shock Doctor webservers (the "Incident"). The code may have targeted certain personal information of customers including those customers' first and last names, billing or mailing addresses, e-mail addresses and credit card information (card holder names, credit card account numbers, expiration months and years and card security codes). (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / NY AG' Author:
Article Title: Shock Doctor
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Shock%20Doctor,%20Inc%20SBN%20to%20Consumer

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-06	**Confluence Charter Schools**	MO	4/24/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

It's important to make you aware of recent concerns regarding the computer network for Confluence Charter Schools. This weekend, the network servers were hacked, which has had an impact on email, phones, SISFIN, our financial system; and Infinite Campus, our student information system.

Attribution 1 Publication: School website / databreaches.net Author:
Article Title: Confluence Charter Schools
Article URL: http://www.confluenceacademy.org/apps/news/article/702340

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-05	**Larimer County Clerk and Recorder's Office**	CO	5/8/2017	Electronic	Government/Military	Yes - Unknown #	**Unknown**

The Larimer County Clerk and Recorder's office made sweeping changes to how it conducts business amid a Denver7 investigation, which revealed how officials had published sensitive information belonging to thousands of people online for months. Among the records were child support liens, death certificates, and commercial lending filings. Many of them contained a variation of social security numbers and dates of birth -- the types of information that would be valuable to identity thieves.

Attribution 1
Publication: denverchannel.com Author:
Article Title: Thousands potentially exposed to identity theft after county published sensitive information online
Article URL: http://www.thedenverchannel.com/news/investigations/thousands-exposed-to-identity-theft-after-county-officials-publi

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-04	**New York City Health and Hospitals Corporation -**	NY	5/9/2017	Paper Data	Medical/Healthcare	Yes - Published #	**3,494**

New York City Health and Hospitals Corporation - Coney Island Hospital NY Healthcare Provider 3494 05/09/2017 Unauthorized Access/Disclosure Other, Paper/Films

Attribution 1
Publication: hhs.gov / hipaajournal.com Author:
Article Title: New York City Health and Hospitals Corporation - Coney Island Hospital
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=22A872E4B360A8A876600506D2D3F371

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-03	**Spine Specialist**	NJ	4/28/2017	Electronic	Medical/Healthcare	Yes - Published #	**600**

Spine Specialist NJ Healthcare Provider 600 04/28/2017 Theft Laptop

Attribution 1
Publication: hhs.gov Author:
Article Title: Spine Specialist
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=22A872E4B360A8A876600506D2D3F371

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-02	**Bronx-Lebanon Hospital / iHealth Solutions**	NY	5/9/2017	Electronic	Medical/Healthcare	Yes - Published #	**7,000**

On May 3, Bob Diachenko of the Kromtech (MacKeeper) Security Research Center contacted me after finding what appeared to them to be tens of thousands or even millions of patients' records exposed due to yet another misconfigured rsync backup. Vendor's error appears to have exposed personal and confidential medical data of patients seen at Bronx-Lebanon Hospital Center since 2014. Records also include addiction histories, psych histories, and histories of physical or sexual abuse.

Attribution 1
Publication: databreaches.net / beckershospitalrevie Author:
Article Title: Confidential medical records from Bronx-Lebanon Hospital exposed online by vendor's error
Article URL: https://www.databreaches.net/confidential-medical-records-from-bronx-lebanon-hospital-exposed-online-by-vendors-e

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170510-01	**True Health Diagnostics**	TX	5/9/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

True Health Diagnostics, based in Frisco, Texas, recently become aware that patients could potentially access the health records of other patients through a security flaw on the company's patient web portal.

Attribution 1
Publication: healthcareinfosecurity.com / krebsonsec Author:
Article Title: Patient Portal Flaw Exposes Lab Records
Article URL: http://www.healthcareinfosecurity.com/patient-portal-flaw-exposes-lab-records-a-9904?rf=2017-05-10_ENEWS_SUB_HI

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170509-08	Pratt Industries	GA	4/28/2017	Electronic	Business	Yes - Published #	7,569

On April 19,2017 a phishing attack directed at Pratt Industries resulted in the disclosure of your first and last name, Social Security number and compensation information. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170509-07	Diamond Institute for Infertility and Menopause	NJ	4/28/2017	Electronic	Medical/Healthcare	Yes - Published #	14,633

On February 27, 2017, we discovered that an unknown individual had gained access to the third-party server containing our electronic health records database. Although the database and your electronic health records were encrypted and remain secure, certain support documents may have been accessible.

Attribution 1 Publication: VT AG's office / hipaajournal.com / NH A Author:
Article Title: Diamond Institute for Infertility and Menopause
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Diamond%20Institute%20for%20Infertility%20and%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170509-06	Horizon Media	NY	4/28/2017	Electronic	Business	Yes - Unknown #	Unknown

Regrettably, on or about March 30, 2017, an employee of Horizon Media, Inc. ("Horizon") was the target and victim of a sophisticated phishing attack by an unknown, unauthorized third party. The records may have contained your name, home address, and social security number. If you are an employee of Horizon, the records may have also included contact information, salary information, and the bank routing number designated by you for direct deposit.

Attribution 1 Publication: VT AG's office Author:
Article Title: Horizon Media
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Horizon%20Media_%20Inc%20SBN%20to%20Consume

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170509-05	Seattle Housing Authority	WA	4/25/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

On March 17, 2017 SHA discovered that the building that houses its housing inspectors had been burglarized and two laptop computers had been stolen. These files may have included client names, addresses, and Social Security numbers.

Attribution 1 Publication: WA AG's office / ME AG's office / ME A Author:
Article Title: Seattle Housing Authority
Article URL: http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Home/Supporting_Law_Enforcement/SeattleHousingAutho

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170509-04	LSU Healthcare Network - New Orleans	LA	5/9/2017	Electronic	Government/Military	Yes - Published #	2,200

The medical data of 2,200 patients of Louisiana State University Health New Orleans were stored on a portable hard drive that was stolen from the Department of Neurology Research in March. Officials do not believe any data on the drive have been misused, although the possibility that ePHI has been viewed cannot be ruled out.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: Unencrypted Hard Drive Stolen from LSU Health New Orleans: 2,200 Individuals Impacted
Article URL: http://www.hipaajournal.com/unencrypted-hard-drive-stolen-from-lsu-health-new-orleans-2200-individuals-impacted-8

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170509-03	Tampa Bay Surgery Center (TDO)	FL	5/9/2017	Electronic	Medical/Healthcare	Yes - Published #	25,848

Aesthetic Dentistry of New York City, OC Gastrocare of Anaheim, CA, and Tampa Bay Surgery Center in Tampa, FL have all had highly sensitive patient data published online last week . The data of 3,496 patients of Aesthetic Dentistry, 34,100 patients of OC Gastrocare, and 134,000 patients of Tampa Bay Surgery Center can now be freely downloaded. A link to the website where the data were dumped was sent out by TDO on Twitter last week. (Number of records per HHS)

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 180,000 Patient Records Dumped Online by The Dark Overlord
Article URL: http://www.hipaajournal.com/180000-patient-records-dumped-online-by-the-dark-overlord-8800/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170509-02	OC Gastrocare (TDO)	CA	5/9/2017	Electronic	Medical/Healthcare	Yes - Published #	34,100

Aesthetic Dentistry of New York City, OC Gastrocare of Anaheim, CA, and Tampa Bay Surgery Center in Tampa, FL have all had highly sensitive patient data published online last week . The data of 3,496 patients of Aesthetic Dentistry, 34,100 patients of OC Gastrocare, and 134,000 patients of Tampa Bay Surgery Center can now be freely downloaded. A link to the website where the data were dumped was sent out by TDO on Twitter last week.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 180,000 Patient Records Dumped Online by The Dark Overlord
Article URL: http://www.hipaajournal.com/180000-patient-records-dumped-online-by-the-dark-overlord-8800/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170509-01	Aesthetic Dentistry of New York City (TDO)	NY	5/9/2017	Electronic	Medical/Healthcare	Yes - Published #	3,496

Aesthetic Dentistry of New York City, OC Gastrocare of Anaheim, CA, and Tampa Bay Surgery Center in Tampa, FL have all had highly sensitive patient data published online last week . The data of 3,496 patients of Aesthetic Dentistry, 34,100 patients of OC Gastrocare, and 134,000 patients of Tampa Bay Surgery Center can now be freely downloaded. A link to the website where the data were dumped was sent out by TDO on Twitter last week.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 180,000 Patient Records Dumped Online by The Dark Overlord
Article URL: http://www.hipaajournal.com/180000-patient-records-dumped-online-by-the-dark-overlord-8800/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170508-02	Wayne Township Board of Education	NJ	5/5/2017	Electronic	Educational	Yes - Unknown #	Unknown

The school district is providing protection to employees following a data breach and phishing scam. "The breach contained personal information about employees and dependents of the Wayne Township Board of Education who received healthcare benefits from the school district," said district Superintendent Dr. Mark Tobak.

Attribution 1 Publication: northjersey.com Author:
Article Title: Wayne schools report data breach, phishing scam
Article URL: http://www.northjersey.com/story/news/passaic/wayne/2017/05/05/wayne-schools-report-data-breech-phishing-scam/3

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170508-01	Greenway Health	FL	5/2/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Tampa, Florida-based practice management software and EHR vendor, Greenway Health, has experienced a ransomware attack that has affected around 5% of its client base – approximately 400 healthcare organizations.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Greenway Health Ransomware Attack Stops 400 Clients from Accessing EHRs
Article URL: http://www.hipaajournal.com/greenway-health-ransomware-attack-stops-400-clients-accessing-ehrs-8790/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-22	GKIC	IL	2/28/2017	Electronic	Business	Yes - Unknown #	Unknown

The incident occurred on February 21 , 2017, when an e-mail that was designed to appear to be from a member of the Company's senior management was sent to an employee in the Company's payroll department instructing the employee to transmit all 2016 W-2 information for review

Attribution 1 Publication: MD AG's office Author:
Article Title: GKIC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280211.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-21	Federal Direct Tax Services	IN	2/28/2017	Electronic	Business	Yes - Published #	258

Specifically, on or about February 2, 2017, Federal Direct discovered that an unauthorized third party launched a cyberattack to attempt to gain electronic access to a group of our partners' Electronic Return Originator (ERO) information. The ERO information that was involved in the incident is attributed to Electronic Filing Identification Number (EFIN) owners, and the unauthorized party potentially accessed your first and last name, date of birth, and Social Security number. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Federal Direct Tax Services
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280210.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-20	DiCentral Corporation	TX	2/27/2017	Electronic	Business	Yes - Unknown #	Unknown

On 23rd February 2017 our team identified a W2 phishing scam. This phishing scam has impacted all employees who received a W2 from DiCentral's USA office for the 2016 calendar year.

Attribution 1 Publication: MD AG's office Author:
Article Title: DiCentral Corporation
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280430.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-19	Piedmont Virginia Community College	VA	3/1/2017	Electronic	Educational	Yes - Unknown #	Unknown

We learned on February 13, 2017, that a PVCC student unintentionally gained access online to a file with various items of your student information. The student notified the College immediately and we removed the file from the web server. nformation in the file included your name, address, Social Security number, and student identification number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Piedmont Virginia Community College
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280425.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-18	ENT of Georgia, LLC	GA	3/2/2017	Electronic	Medical/Healthcare	Yes - Published #	383

On October 31 2016, ENT of GA's retirement plan web portal was the focus of a phishing attack which may have resulted in an unknown individual gaining access to employee retirement plan accounts. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: ENT of Georgia, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280435.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-17	Atlantic Coast Mortgage	VA	3/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On February 15, 2017, we learned that one of our employees had received a phishing email in January, designed to appear as if it came from our CEO, and the employee responded to the email on January 24, 2017.

Attribution 1 Publication: MD AG's office Author:
Article Title: Atlantic Coast Mortgage
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280427.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-16	Capital Nephrology	MD	5/2/2017	Electronic	Medical/Healthcare	Yes - Published #	4,000

Capital Nephrology MD Healthcare Provider 4000 05/02/2017 Hacking/IT Incident Electronic Medical Record, Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Capital Nephrology
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=7AFBCE100CAB3F5475DD63545F23E4B5

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-15	Humana Inc. (#HU17001CC)	KY	4/18/2017	Electronic	Medical/Healthcare	Yes - Published #	3,831

Humana Inc [case # HU17001CC] KY Health Plan 3831 04/18/2017 Hacking/IT Incident Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Humana Inc. (#HU17001CC)
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=7AFBCE100CAB3F5475DD63545F23E4B5

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-14	REI Holding Co.	FL	4/20/2017	Electronic	Business	Yes - Published #	638

On March 6, 2017, REI discovered that the HR manager's business laptop had been stolen. REI determined that the laptop may have contained the names, addresses, dates of birth, 401 K account information, Social Security numbers, and tax information of current and former employees, employee family members, and applicants. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: REI Holding Co.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/rei-holding-20170420.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-13	KeraLink International	MD	4/25/2017	Electronic	Business	Yes - Published #	202

We recently discovered that our company was the victim of an email spoofing attack on April 6, 2017, by an individual pretending to be our Chief Executive Officer. A request was made for all 2016 KeraLink International employee W-2 information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / ME AG Author:
Article Title: KeraLink International
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/keralink-20170425.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-12	Connecticut College	CT	4/10/2017	Electronic	Educational	Yes - Unknown #	Unknown

On January 20, 2017, an employee responded to an email by clicking a link within the message that compromised the email account. Based on the comprehensive investigation and document review, Connecticut College has confirmed that the compromised email account contained full name, address, date of birth, and may have included Social Security
number or state ID/driver's license number.

Attribution 1 Publication: NH AG's office Author:
Article Title: Connecticut College
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/connecticut-college-20170410.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-11	CuttersSports / Nathan Sports	CA	5/1/2017	Electronic	Business	Yes - Published #	2,098

On April 11 , 2017, Cutters discovered the personal information of twenty (20) New Hampshire residents may have been affected when an external actor or actors placed hidden code on the Cutters webservers (the "Incident"). The code may have targeted certain personal information of customers who made credit card purchases via the Cutters webservers, including those customers' first and last names, billing or mailing addresses, e-mail addresses and credit card information (card holder names, cred it card account numbers, expiration months and years and card security codes). (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: CuttersSports / Nathan Sports
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/cuttersports-20170501.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-10	Berard & Associates	NY	4/6/2017	Electronic	Business	Yes - Published #	575

On or about February 13, 2017, we learned that documents stored on our vendor SmartVault's portal had been accessed by an unauthorized party using the log-in credentials of a Berard & Associates employee. Due to the nature of financial documents maintained on the SmartVault system , the documents that were accessed without authorization contained the names, addresses, dates of birth , social security numbers and/or financial account numbers of our clients and/or their spouses and dependents. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Berard & Associates
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/berard-20170406.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-09	Thirty-One Gifts	OH	4/28/2017	Electronic	Business	Yes - Unknown #	Unknown

We recently discovered unauthorized access to one of our employee's email accounts which contained documents with portions of your personal information. Although our investigation is ongoing, we have determined that the personal information involved in this incident may have included your name, payment card account number, and shipping address.

Attribution 1 Publication: VT AG's office / NY AG's office Author:
Article Title: Thirty-One Gifts
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Thirty-One%20Gifts%20LLC%20SBN%20to%20Consum

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-08	Paint Nite LLC	MA	4/28/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 8, 2017, a Paint Nite LLC ("Paint Nite") employee was sending out a blank Excel template to six licensees to fill out. Inadvertently, a second tab in the worksheet was included in the email. The second tab contained the name, addresses and financial account/bank information of Paint Nite licensees.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-07	Sabre Hospitality Solutions / SynXis / 36,000 Hotels	TX	5/4/2017	Electronic	Business	Yes - Unknown #	Unknown

"We are investigating an incident involving unauthorized access to payment information contained in a subset of hotel reservations processed through the Sabre Hospitality Solutions SynXis Central Reservation system."

Attribution 1 Publication: esecurityplanet.com Author:
Article Title: Sabre Hospitality Solutions / SynXis / 36,000 Hotels nationwide
Article URL: http://www.esecurityplanet.com/network-security/sabre-breach-may-have-exposed-payment-data-at-36000-hotels.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-06	**Zinc Auto Finance, Inc.**	CA	5/3/2017	Electronic	Business	Yes - Unknown #	**Unknown**

This letter is written to inform you, that on August 21, 2017 we became aware of an employee who accessed your account information without a direct business need. The account information could have included name, date of birth, home address, phone number, Social Security Number and Credit/Debit card information.

Attribution 1 Publication: CA AG's office Author:
Article Title: Zinc Auto Finance, Inc.
Article URL: https://oag.ca.gov/system/files/Sample%20Notice%20of%20Breach%20uploaded%20to%20Secretary%20of%20State_0.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-05	**MSA Accounting, CPA Professional Corp.**	CA	5/2/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We are writing to provide you with information about suspicious activity involving some MSA Accounting, CPA Professional Corp. clients. If you are an individual, this information on our system may have included your: name, date of birth,telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), direct deposit bank account information (including account number and routing information if provided to us), and any supporting documents you may have provided including health care.

Attribution 1 Publication: CA AG's office Author:
Article Title: MSA Accounting, CPA Professional Corp.
Article URL: https://oag.ca.gov/system/files/Ahluwalia%20Letter%20Version%201_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-04	**McDavid, Inc.**	IL	4/28/2017	Electronic	Business	Yes - Published #	**4,777**

On April 6, 2017, McDavid discovered that your personal information may have been affected when an external actor or actors placed hidden code on the McDavid webservers (the “Incident”). (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / VT AG' Author:
Article Title: McDavid, Inc.
Article URL: https://oag.ca.gov/system/files/McDavid%20CA%20Sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-03	**Nova Southeastern University**	FL	5/1/2017	Electronic	Educational	Yes - Published #	**1,086**

On March 2, 2017, we learned that two unencrypted portable hard drives were stolen from an NSU employee on February 28, 2017. Our investigation determined that the hard drives contained information related to an NSU laboratory and included your name, provider’s name, and lab result. Your social security number and other financial information were not contained on the drives.

Attribution 1 Publication: MT AG's office / hhs.gov Author:
Article Title: Nova Southeastern University
Article URL: https://dojmt.gov/wp-content/uploads/Nova-Southeastern-University.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-02	**Texas Yale Capital Corp. dba Yale Capital Corp.**	FL	4/6/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**116**

Between February 21 and March 3, 2017, unauthorized persons gained accessed to Texas Yale Capital Corp. d.b.a. Yale Capital Corp.'s ("YCC") computer system which stored its clients' personal information. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / VT AG's office / NY AG' Author:
Article Title: Texas Yale Capital Corp. dba Yale Capital Corp.
Article URL: https://dojmt.gov/wp-content/uploads/Yale-Capital-Corp.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170504-01	Agri Beef / Snake River Farms	ID	5/2/2017	Electronic	Business	Yes - Published #	7,933

Gorilla Group, a third-party partner that hosts Snake River Farms servers, advised us that a data security incident occurred during the window of November 22, 2016 to April 4, 2017, and Gorilla Group notified Agri Beef of the incident on April 5, 2017. During the window, a third party may have gained access to snakeriverfarms.com with the intent to obtain certain PII. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / CA AG's office / NY AG' Author:
Article Title: Agri Beef / Snake River Farms
Article URL: https://dojmt.gov/wp-content/uploads/Agri-Beef.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170502-08	Merchants Metals, Inc.	GA	3/1/2017	Electronic	Business	Yes - Published #	759

On February 27, 2017, Merchants Metals learned that it had been the target of a spear phishing email scam perpetrated upon the company. As a result, on February 1, 2017, an employee inadvertently c-mailed a PDF version of employee 2016 W-2 forms to an unauthorized individual. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Merchants Metals, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280432%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170502-07	KOMAN Government Solutions	MA	4/21/2017	Electronic	Business	Yes - Unknown #	Unknown

This letter follows KOMAN Government Solutions, LLC's (the "Company") prior telephonic communications with its employees immediately following its discovery of a data security incident that may have involved employee personal information.

Attribution 1 Publication: VT AG's office Author:
Article Title: KOMAN Government Solutions
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/KOMAN%20Government%20Solutions%20LLC%20SBN

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170502-06	MOTL Accounting	IL	4/25/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 16, 2017, we discovered that information from your 2010 tax return that was stored on our server may have been accessed by an unknown, unauthorized third-party.

Attribution 1 Publication: MT AG's office Author:
Article Title: MOTL Accounting
Article URL: https://dojmt.gov/wp-content/uploads/Motl-Marketing.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170502-05	Pacific Quest	CA	4/27/2017	Electronic	Business	Yes - Published #	319

We have become aware of our victimization through a criminal email phishing scam that has compromised full names, social security numbers and wage information. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office / ME AG Author:
Article Title: Pacific Quest
Article URL: https://dojmt.gov/wp-content/uploads/Pacific-Quest.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170502-04	Memorial Hospital Clinic West	TX	4/26/2017	Electronic	Medical/Healthcare	Yes - Published #	521

Memorial Hospital Clinic West TX Healthcare Provider 521 04/26/2017 Hacking/IT Incident Electronic Medical Record, Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Memorial Hospital Clinic West
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170502-03	Memorial Hospital Clinic South	TX	4/26/2017	Electronic	Medical/Healthcare	Yes - Published #	842

Memorial Hospital Clinic South reported a breach when computer malware (i.e.,ransomware) was found on its network server. This breach affected the protected health information (PHI) of 842 individuals, and included clinical and demographic information. The specific types of PHI involved in the breach included addresses, birthdates, driver's license numbers, names, social security numbers, diagnoses/conditions, lab results, medications, and other treatment information. This review has been consolidated with another review of this covered entity.

Attribution 1 Publication: hhs.gov Author:
Article Title: Memorial Hospital Clinic South
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170502-02	Eyecare Services Partners Management, LLC	TX	4/12/2017	Electronic	Medical/Healthcare	Yes - Published #	9,129

Eyecare Services Partners Management, LLC TX Business Associate 9129 04/12/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Eyecare Services Partners 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
ITRC20170502-01	Area Agency of Aging 1-B	MI	4/13/2017	Electronic	Medical/Healthcare	Yes - Published #	1,741

Area Agency of Aging 1-B MI Healthcare Provider 1741 04/13/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Area Agency of Aging 1-B
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-13	Donaldson Company, Inc.	MN	4/24/2017	Electronic	Business	Yes - Unknown #	Unknown

Donaldson employee's company-issued laptop containing personal information related to you and others was stolen from a personal vehicle on March 24, 2017. The incident involved the following information: your name, address, birthdate, and Social Security number.

Attribution 1 Publication: NH AG's office / MT AG's office Author:
Article Title: Donaldson Company, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/donaldson-20170424.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-12	Greenwood County School District 50	SC	4/28/2017	Electronic	Educational	Yes - Published #	3,300

About 3,300 people might be affected by a security breach after an unauthorized user logged in to four Greenwood County School District 50 employees' emails as well as current and former employees' payroll accounts in January and February.

Attribution 1 Publication: indexjournal.com / ME AG's office Author:
Article Title:
Article URL: http://www.indexjournal.com/news/d-notifies-parents-staff-about-data-breach/article_24602c10-5e93-58f4-a13b-6b680d

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-11	**Pentucket Medical**	MA	4/29/2017	Paper Data	Medical/Healthcare	Yes - Unknown #	**Unknown**

It seems that on January 18, four boxes of mainly physician/clinician records were removed from CubeSmart Storage Facility by another client of the facility. Employee information in the files included and last names, addresses, employment contracts, Social Security numbers and compensation information. Information on an unspecified number of patients included their names, Social Security numbers, and health insurance information.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: Pentucket Medical notifies employees and patients of data security incident
Article URL: https://www.databreaches.net/pentucket-medical-notifies-employees-and-patients-of-data-security-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-10	**AMP**	IL	4/26/2017	Electronic	Business	Yes - Unknown #	**Unknown**

A data breach at an online futures trading brokerage left exposed thousands of files, including credit reports, passport scans, and customer chat logs.

Attribution 1 Publication: dailydot.com Author:
Article Title: Data breach at online trading firm exposed customer credit reports, Social Security numbers
Article URL: https://www.dailydot.com/layer8/amp-trading-firm-data-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-09	**Alliance Direct Lending Corporation**	CA	4/27/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**500,000**

The researchers discovered what appears to be customer purchase information, including full names, addresses, FICO credit scores, vehicle information, and the last four digits of Social Security numbers. Additionally, several audio recordings were leaked of conversations between the customers and lenders, both in Spanish and English—the “consent calls” included the customers’ names, dates of birth, Social Security numbers, and phone numbers.

Attribution 1 Publication: dailydot.com Author:
Article Title: Data breach of U.S. auto lender left over 500K customers exposed
Article URL: https://www.dailydot.com/layer8/alliance-direct-lending-corporation-data-breach-fixed/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-08	**Harrisburg Gastroenterology Ltd.**	PA	5/1/2017	Electronic	Medical/Healthcare	Yes - Published #	**102,600**

On March 17, 2017, following an investigation of potentially suspicious system activity, we determined that an unauthorized individual could have potentially accessed Harrisburg Gastroenterology’s patient information. The patient information contained in our systems includes your name, demographic information, Social Security number, health insurance information, diagnostic information, and clinical information. (Exposure number per NY AG's office)

Attribution 1 Publication: company website / hhs.gov / NY AG's of Author:
Article Title: Harrisburg Gastroenterology Ltd.
Article URL: https://www.hbggastro.com/

Attribution 2 Publication: lancasteronline.com Author:
Article Title: Two Central PA medical practices report potential data breach
Article URL: http://lancasteronline.com/news/local/two-central-pa-medical-practices-report-potential-data-breach/article_b7f5b1bc-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-07	**Harrisburg Endoscopy and Surgery Center, inc.**	PA	5/1/2017	Electronic	Medical/Healthcare	Yes - Published #	**9,092**

On March 17, 2017, following an investigation of potentially suspicious system activity, we determined that an unauthorized individual could have potentially accessed Harrisburg Endoscopy's patient information. The patient information contained in our systems includes your name, demographic information, Social Security number, health insurance information, diagnostic information, and clinical information.

Attribution 1 Publication: company website . MT AG's office / hhs. Author:
Article Title: Harrisburg Endoscopy and Surgery Center, inc.
Article URL: https://www.hbgesc.com/

Attribution 2 Publication: lancasteronline.com Author:
Article Title: Two Central PA medical practices report potential data breach
Article URL: http://lancasteronline.com/news/local/two-central-pa-medical-practices-report-potential-data-breach/article_b7f5b1bc-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-06	Retina-X Studios	FL	5/1/2017	Electronic	Business	Yes - Unknown #	Unknown

A hacker known for SQL exploits of great magnitude was able to find a weakness in a decompiled and decrypted version of a now-discontinued product. The tables held information such as login usernames, subscription keys, device metadata, text messages, GPS locations, contacts' information, apps installed and website logs

Attribution 1 Publication: phonesheriff.com Author:
Article Title: Retina-X Studios Server Breached by Hackers
Article URL: http://www.phonesheriff.com/blog/retina-x-studios-server-breached-by-hackers/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-05	City of Fitchburg	MA	5/1/2017	Electronic	Government/Military	Yes - Published #	1,800

On Aug. 28, 2013 the data was either uploaded to the internet "as a result of a hack," or accidentally removed from the hard drive of a former city employee's computer, according to a report filed by the city with the Office of Consumer Affairs and Business Regulation.

Attribution 1 Publication: sentinelandenterprise.com Author:
Article Title: Authorities just learn of 2013 breach of Fitchburg city records that releases Social Security numbers of 1,800 state residents
Article URL: http://www.sentinelandenterprise.com/breakingnews/ci_30958648/authorities-just-learn-2013-breach-fitchburg-city-rec

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-04	Chipotle Mexican Grill	CO	4/27/2017	Electronic	Business	Yes - Unknown #	Unknown

While it's not yet clear how the Chipotle breach occurred, Hart said, hackers often hit payment networks by stealing employees' or third-party vendors' login credentials. "That's why it's important for companies to not only implement the more secure EMV and encrypt payment data but to make sure there are additional layers of security, such as multi-factor authentication, for the individuals that can access the payment systems and networks," he said.

Attribution 1 Publication: esecurityplanet.com / WI AG's office / C Author:
Article Title: Chipotle Hit by Credit Card Breach
Article URL: https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-03	Hill Country Memorial Hospital	TX	5/1/2017	Electronic	Medical/Healthcare	Yes - Published #	8,449

An unauthorized individual has gained access to an email account of an employee of Hill Country Memorial Hospital and sent a number of fraudulent invoices, but potentially also accessed the protected heath information of certain patients. The email account contained patients' names, addresses, ID numbers, dates of birth, prescription and treatment information, medical diagnoses, procedure information and Social Security Numbers.

Attribution 1 Publication: hipaajournal.com / MT AG's office / VT A Author:
Article Title: Hill Country Memorial Hospital
Article URL: http://www.hipaajournal.com/hill-country-memorial-hospital-discovers-email-account-compromise-8789/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-02	**Gannett Company**	VA	4/28/2017	Electronic	Business	Yes - Published #	**18,100**

On Thursday, March 30, 2017, we discovered that several members of our HR department were victims of a phishing attack that compromised their Office 365 account login credentials, including their Gannett email.Information that may have been available through the impacted employee credentials includes names, contact information, Social Security numbers, dates of birth, bank account numbers, bank routing numbers, dates of employment, salary information, benefits election and insurance policy information, and other related information maintained for HR purposes. (Exposure number per NY AG's office)

Attribution 1 Publication: USAtoday.com / ME AG's offic Author:
Article Title: Gannett hit with email phishing attack
Article URL: https://www.usatoday.com/story/tech/news/2017/05/02/gannett-hit-email-phishing-attack/101200110/

Attribution 2 Publication: CA AG's office / NH AG's office / NY AG' Author:
Article Title: Gannett Company
Article URL: https://oag.ca.gov/system/files/_gannet501_1_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170501-01	**Extreme Reach**	MA	5/1/2017	Electronic	Business	Yes - Published #	**3,800**

On February 8, 2017, a small number of employees were targeted by a phishing email which resulted in those employees' email credentials being compromised. As part of our ongoing investigation, we determined on April 10, 2017, that the following information about you was contained in an email account (or associated cloud drive) at the time of the unauthorized access: Social Security number, driver's license number, financial account number, credit card number, passport number and name. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / ME AG Author:
Article Title: Extreme Reach
Article URL: https://oag.ca.gov/system/files/Extreme%20Reach%20--%20Notice%20only%20--%20CA_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-21	**Neosho County Community College**	KS	3/2/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

On February 17, 2017, NCCC discovered that an employee was the subject of a phishing attack when the employee received an email purporting to be from an executive, requesting copies of employee W -2 wage and tax statements. In response to that email, a spreadsheet of employee W-2 information was sent to an unauthorized email address.

Attribution 1 Publication: MD AG's office Author:
Article Title: Neosho County Community College
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280437.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-20	**Bostwick Laboratories**	VA	3/2/2017	Electronic	Business	Yes - Published #	**269**

On February 22, 2017, Bostwick was the target of an email phishing scam when an employee received a request that appeared to be from a Bostwick Executive, requesting copies of employees' wage and tax statements. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Bostwick Laboratories
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280436%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-19	**Country Financial**	IL	3/3/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

We have reason to believe that a former COUNTRY Financial® agent collected personally identifiable information prior to leaving the company. This former agent was able to view your personal information because he was your servicing agent when this incident occurred in early 2015.

Attribution 1 Publication: MD AG's office Author:
Article Title: Country Financial
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280438.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-18	State Farm Mutual Automobile Insurance	IL	3/2/2017	Electronic	Business	Yes - Published #	10,421

GMR was notified in late October 2016 by a security researcher that he had been able to access electronic files relating to cases in which GMR was representing or had represented parties insured in certain lawsuits or other matters. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: State Farm Mutual Automobile Insurance Company / Goldberg Miller & Rubin
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281052.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-17	Barclay's Bank Delaware	DE	3/6/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

I am writing to notify you of a data security incident that occurred in early January in which suspected unauthorized logins into a number of Barclaycard accounts were detected, affecting one (1) Barclaycard account belonging to a Maryland resident. The unauthorized users may have gained access to the affected customers' names, addresses, and 16-digit credit card numbers (but not other personal identity or credit card information).

Attribution 1 Publication: MD AG's office Author:
Article Title: Barclay's Bank Delaware
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280519%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-16	Community Assistance Network (CAN)	MD	3/6/2017	Electronic	Business	Yes - Unknown #	Unknown

As a result of information inadvertently emailed to an improper recipient, an unknown party is in possession of 2016 W-2's for all CAN employees. This incident involved disclosure of your full name, address, Social Security Number and 2016 wages.

Attribution 1 Publication: MD AG's office Author:
Article Title: Community Assistance Network (CAN)
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280522.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-15	Kobza & Associates, LLC	IL	3/7/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 7, 2017, I received an email from an individual, using the moniker "thedarkoverlord", who claimed to have accessed client information. The unauthorized actor may have illegally accessed information you have provided me. This includes your name; address; Social Security number; FEIN number; phone number; email address; and date of birth. Other information you have provided may also have been accessed, such as: bank and financial account information; tax forms and tax-related information; salary and income information; assets and investment statements; and information related to your dependents and/or beneficiaries.

Attribution 1 Publication: MD AG's office Author:
Article Title: Kobza & Associates, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280524.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-14	INSYS Group	NJ	3/8/2017	Electronic	Business	Yes - Published #	564

On Friday, March 3rd, 2017, INSYS Group was the victim of a phishing attack in which one of our employees e-mailed a document containing your W-2 personal information to an email account fraudulently claiming to be one of our corporate officers. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: INSYS Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280650.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-13	Elkay Plastics Co., Inc.	CA	3/6/2017	Electronic	Business	Yes - Published #	243

Although our investigation has not found any evidence of inappropriate access to any information maintained by Elkay Plastics, we suspect that potentially an unauthorized individual may have obtained IRS Form W -2s for some of our cunent and former employees for tax year 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / ME AG's office / NY AG Author:
Article Title: Elkay Plastics Co., Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280657.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-12	Prince George's County Memorial Library System	MD	2/21/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

One of our employee's accounts was accessed without authorization. We are writing to you because our investigation indicates that at least some W-2 data may have been accessed by the person responsible.

Attribution 1 Publication: MD AG's office Author:
Article Title: Prince George's County Memorial Library System
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280655.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-11	Taconic Biosciences, Inc.	NY	3/8/2017	Electronic	Business	Yes - Published #	665

On or around January 30, 2017, a Taconic employee received, and complied with, an email appearing to come from another Taconic employee requesting the release of W-2 tax information for Taconic employees for the 2016 tax year. Taconic learned on or around February 10, 2017 that the email requesting the W-2 tax data was a "phishing" email from an unauthorized individual. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Taconic Biosciences, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280527%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-10	Frost & Sullivan	TX	3/9/2017	Electronic	Business	Yes - Published #	370

On March 3, 2017, Frost & Sullivan learned that a targeted "spear phishing" email message had been sent to an employee. The information affected by this incident therefore included these employees' names, addresses, Social Security numbers, incomes and tax withholding information. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / ME AG's office / NY AG Author:
Article Title: Frost & Sullivan
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280660.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-09	Matthews, Carter and Boyce	VA	4/4/2017	Electronic	Business	Yes - Unknown #	Unknown

Please be aware that Matthews, Carter and Boyce suffered a security incident on February 9, 2017, where 10 vendors from our client and your employer, Northern Virginia Eye Surgery Center had their 1099-MISC forms placed on a public folder accessible on our computer system that was accessible to other Matthews, Carter and Boyce clients.

Attribution 1 Publication: MD AG's office Author:
Article Title: Matthews, Carter and Boyce
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280662%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-08	GetWellNetwork	MD	3/10/2017	Electronic	Business	Yes - Published #	386

We value the elationship we have with you and the trust you have in us. On March 8, 2017, GetWellNetwork became aware that we have fallen victim to an email phishing scam. Our payroll department was targeted by an isolated scam that impersonated me and requested employee information be sent via email. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: GetWellNetwork
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281088.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-07	Village Green Holdings	MI	3/10/2017	Electronic	Business	Yes - Published #	745

The incident occurred on or around February 9, 2017, when Village Green mailed a zip drive containing unencrypted rental applications of former renters to the current owners of the St. Louis Park apartment building. The rental applications contained the first and last name of the renters along with other personally identifiable information, including social security numbers. Unfortunately, the package was damaged in transit and the zip drive was separated from the package. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / CT AG's office / NY AG' Author:
Article Title: Village Green Holdings
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280756.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-06	Clark Schaefer Hackett	OH	3/10/2017	Electronic	Business	Yes - Published #	1,895

On February 7, 2017, we learned that an unauthorized individual may have gained access to an employee's email account. When we learned of this, we immediately secured the email account, reset passwords and began an investigation of the incident. We conducted a thorough review of the employee's e-mail account and confirmed that the emails contained some personal information and may have included your name, address, date of birth, and Social Security number. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Clark Schaefer Hackett
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280918.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-05	Atlas Container Corporation	MD	3/7/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 1, 2017, Atlas Container discovered that on February 21, 2017, as a result of a criminal phishing email, an unauthorized third party obtained an electronic file containing dates of birth and 2016 Form W-2s of current and some former employees of Atlas Container.

Attribution 1 Publication: MD AG's office Author:
Article Title: Atlas Container Corporation
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281074.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-04	Vectorworks, Inc.	MD	3/13/2017	Electronic	Business	Yes - Unknown #	Unknown

On Friday, March 3, 2017, a fraudulent individual contacted Vectorworks from an e-mail address similar to our own Vectorworks domain name. The email used Vectorworks language, was not outside of an ordinary
request and was timely as we were finishing pay raise letters on that day. For active employees, at December 31, 2016: Employee Name, Social Security Number, Address, Salary and Date of Birth.

Attribution 1 Publication: MD AG's office Author:
Article Title: Vectorworks, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281089%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-03	Faller, Kincheloe & Co., PLC	IA	3/13/2017	Electronic	Business	Yes - Published #	3,430

FKC believes this data security incident was connected to a malicious hacking that occurred on February 4, 2017. On that day, FKC lost access to its information system. The information which may have been involved includes tax return information, including names, addresses, dates of birth, social security numbers, and bank account numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Faller, Kincheloe & Co., PLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280921%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-02	Pro-Vigil	TX	3/15/2017	Electronic	Business	Yes - Published #	237

On or about March 13, 2017, an incident occurred that allowed an unknown individual to obtain year-end tax reporting information using a fictitious or “spoofed” e-mail. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / CT AG's office / NY AG' Author:
Article Title: Pro-Vigil
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280931%20(2).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170428-01	Schulman Rogers	MD	3/13/2017	Electronic	Business	Yes - Unknown #	Unknown

On Feburary 27, 2017, we discovered unauthorized access to one employee record via email "spoofing" from an unauthorized user. Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. As a result of this criminal act, the unauthorized access resulted in the release of information that we store in connection with tax preparation, including name, address and the employee's social security number.

Attribution 1 Publication: MD AG's office Author:
Article Title: Schulman Rogers
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281057.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-15	Western Health Screening	MT	4/22/2017	Electronic	Medical/Healthcare	Yes - Published #	15,326

WHS recently learned that a vehicle owned by WHS in route to a Health Fair and passing through Salt Lake City, Utah, was stolen. There was a piece of computer equipment known as a “jump drive” belonging to WHS that was in the stolen vehicle. Upon learning of this theft, WHS immediately investigated and determined that the jump drive, which was password protected, but unencrypted, contained participants’ personal information.

Attribution 1 Publication: healthitsecurity.com Author:
Article Title: Stolen, Unencrypted Drive Causes Data Security Concern for 15K
Article URL: http://healthitsecurity.com/news/stolen-unencrypted-drive-causes-data-security-concern-for-15k

Attribution 2 Publication: databreaches.net / WHS website Author:
Article Title: Western Health Screening
Article URL: http://whs.cc/wp-content/uploads/2017/04/119407-Western-Health-Screening-Letter.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-14	Los Angeles City Employees' Retirement System	CA	4/5/2017	Electronic	Business	Yes - Unknown #	Unknown

We recently learned that an email attachment containing personally identifiable information was accessed by one individual who received it inadvertently from a LACERS’ staff member.

Attribution 1 Publication: CA AG's office Author:
Article Title: Los Angeles City Employees' Retirement System
Article URL: https://oag.ca.gov/system/files/DataBreachLetter%20040517%20-%20Final_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-13	**LookingGlass Cyber Solutions**	VA	3/15/2017	Electronic	Business	Yes - Published #	**369**

On Tuesday, March 14, 2017 LookingGlass became aware that we have fallen victim to a Business Email Compromise (BEC). Our human resources department was targeted by an isolated scammer who requested specific employee information be sent via email reply. It did not target or affect our users, systems, clients or service whatsoever. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: LookingGlass Cyber Solutions
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280960%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-12	**Aisthesis**	MD	3/16/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

We are writing as a follow up to our letter, dated March 8, 2017, informing you that Aisthesis was the victim of an email phishing scheme, which resulted in an unauthorized party obtaining a copy of your 2016 W-2 form, which included your name, address, SSN and 2016 compensation information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Aisthesis
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280963.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-11	**Allegis Group / Talx**	MD	3/6/2017	Electronic	Business	Yes - Published #	**40,645**

We are writing to tell you about a data security incident involving the unauthorized access to electronic copies of your W-2 tax form. A user reset the PIN to access your account through the online portal and then accessed your online account on [date]. Afterward, Talx determined that this PIN reset and account access was unauthorized. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's offce / MD AG' Author:
Article Title: Allegis Group / Talx
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281065.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-10	**AFLAC / Continental American Insurance Company**	SC	3/16/2017	Electronic	Business	Yes - Unknown #	**Unknown**

I am writing in accordance with the MD. Code Ann. Comm. Law 14-3504 to inform you of an incident that was reported to us by one of our 1099 independent contractors. The business associate used by Continental American Insurance Company (CAIC) fell victim to a ransomware email attack. This resulted in the possible visibility of insured personal and financial information, including Social Security Numbers and banking information.

Attribution 1 Publication: MD AG's office Author:
Article Title: AFLAC / Continental American Insurance Company
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280959%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-09	**TIC Gums, Inc. / Specialty Blends, Inc.**	MD	3/17/2017	Electronic	Business	Yes - Published #	**268**

TIC discovered on March 10, 2017 that a successful phishing attack on February 27, 2017 resulted in the unauthorized disclosure of W-2 information for 2015 and 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: TIC Gums, Inc. / Specialty Blends, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280965%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-08	American Pest	CA	3/20/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 3, 2017 we discovered that ea rlier that same day, as a result of a criminal phishing email, an unauthorized third party obtained an electronic file containing 2015 and 2016 Form W-2s of certain current and former employees of American Pest.

Attribution 1 Publication: MD AG's office Author:
Article Title: American Pest
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281073.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-07	Jackson College	MI	3/21/2017	Electronic	Educational	Yes - Published #	438

On February 16, 2017, JC discovered that certain potentially sensitive data was accessible through JC's local campus directory and that the data had been inadvertently viewed by a current JC student. The information contained in the directory may have included your loved one's name, Social Security number, JC username and password, email address, JC identification number, and date of birth. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Jackson College
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280972.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-06	Refund Advantage / A Division of MetaBank	KY	3/21/2017	Electronic	Banking/Credit/Financial	Yes - Published #	4,147

On March 3, 2017, we identified that unknown thieves stole the user names and passwords used by your tax preparers to access electronic records stored on a Refund Advantage system. Your tax preparer's file included your name, address, date of birth, social security number, and bank account information. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Refund Advantage / A Division of MetaBank
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281090.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-05	National Safety Council	IL	3/21/2017	Electronic	Business	Yes - Unknown #	Unknown

On or about March 13, 2017, two NSC emails, each with an attachment that included personal information about NSC employees, was erroneously sent in response to an email request that appeared to be valid. On or about March 14, 2017, we concluded that these emails were likely sent to an unauthorized recipient.

Attribution 1 Publication: MD AG's office Author:
Article Title: National Safety Council
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280970.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-04	Monoflo International	VA	3/23/2017	Electronic	Business	Yes - Unknown #	Unknown

Monoflo was the victim of an email spoofing attack on March 1, 2017, by an individual pretending to be a Monoflo executive. A request was made from what appeared to be a legitimate Monoflo email address for all 2016 Monoflo employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before the company discovered that the request was made from a fraudulent account by someone using the name and email address that appeared to be from a Monoflo executive.

Attribution 1 Publication: MD AG's office Author:
Article Title: Monoflo International
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280974.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-03	**VT industries**	IA	3/24/2017	Electronic	Business	Yes - Published #	**1,884**

VT Industries recently learned that an unauthorized individual, impersonating a VT Industries executive, contacted a VT Industries employee requesting access to its cloud-based Human Resources Information System. Before it was determined that the request was fraudulent, the employee provided access to the system that contained limited information about some of its employees, including first and last name, address, Social Security number, and 2016 compensation information. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: VT industries
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281068.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-02	**IntelePeer Holdings**	CA	3/23/2017	Electronic	Business	Yes - Published #	**213**

On February 1, 2017, an unauthorized individual, impersonating a member of IntelePeer, contacted an IntelePeer employee requesting company employee W-2 information. Without realizing that the request was fraudulent, the employee provided files containing limited information about some of IntelePeer's current and former employees. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / ME AG's office / NY AG Author:
Article Title: IntelePeer Holdings
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281071.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170425-01	**Elwood Staffing**	IN	3/24/2017	Electronic	Business	Yes - Published #	**6,011**

On Wednesday, February 22, 2017, Elwood learned that an employee sent a series of emails from a company issued email account to a personal Yahoo email account. Some of the emails, sent on February 21, 2017, included spreadsheets with lists of information that included personally identifiable information, including name and social security number. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Elwood Staffing
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280174.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-35	**Vertical Bridge**	FL	3/27/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On March 7, 20I7, we learned that, on February I, 20I7 an employee responded to an email that appeared to be, but was not from a senior executive. The response provided W-2 information.

Attribution 1 Publication: MD AG's office Author:
Article Title: Vertical Bridge
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280982.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-34	**ABS Associates, Inc.**	IL	3/20/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We recently learned that on February 9, 2017, ABS Associates was the victim of a nation-wide phishing attack that resulted in the disclosure of ABS's 2016 W-2 Forms. ·

Attribution 1 Publication: MD AG's office Author:
Article Title: ABS Associates, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281067.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-33	Clean Advantage / Advantage Waste Removal	MD	3/28/2017	Electronic	Business	Yes - Unknown #	Unknown

Information obtained from the 2016 W-2s was been breached on Monday, March 27, 2017. Due to this, social security numbers may have been compromised.

Attribution 1 Publication: MD AG's office Author:
Article Title: Advantage Waste Removal
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280985.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-32	Toole Design Group, LLC	MD	3/29/2017	Electronic	Business	Yes - Unknown #	Unknown

Our HR Coordinator (Kay) got a phishing email on Tuesday, March 28 asking her to forward our W-2's for 2016 to a fraudulent email address. She forwarded that information without confirming that the email was real.

Attribution 1 Publication: NY AG's office Author:
Article Title: Toole Design Group, LLC
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-31	Cross Street Partners	MD	3/29/2017	Electronic	Business	Yes - Unknown #	Unknown

We're sorry to have to inform you that we have just learned that Cross Street Partners has been the victim of an internet scam, and some confidential information- the employee 2016 W2's - were fraudulently obtained.

Attribution 1 Publication: MD AG's office Author:
Article Title: Cross Street Partners
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281091.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-30	CFG / Capital Funding Group	MD	3/24/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On March 17, 2017, CFG was the victim of an email spoofing attack by an individual or individuals pretending to be CFG's Owner. The fraudulent email requested 2016 CFG employee W-2 information. A list containing names, Social Security numbers, and year to date earnings from 2016 employee W-2 forms was provided before the company discovered that the request was fraudulent.

Attribution 1 Publication: MD AG's office Author:
Article Title: Capital Funding Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280990.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-29	Jeffrey S. Steiner, CPA	FL	3/31/2017	Electronic	Business	Yes - Published #	223

On or about March 8, 2017, Jeffrey s. Steiner, CPA, PA became aware that it was the victim of a cyber-attack bv which an unknown third party was able to access Jeffrey s. Steiner, CPA, PA's computer network and some of its clients' personal information. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: Jeffrey S. Steiner, CPA
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280500.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-28	Connections Therapy Center	DC	3/30/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 16, 2017, The Connections Therapy Center was the target of an email phishing scam that resulted in the unauthorized disclosure of our 2016 employees' private information. Specifically, 2016 W-2 tax information for all Company employees was released, including their names, social security numbers and compensation amounts, for current and former employees who received compensation from the Company during 2016.

Attribution 1 Publication: MD AG's office Author:
Article Title: Connections Therapy Center
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280504.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-27	ACSIA Partners	WA	3/30/2017	Electronic	Business	Yes - Published #	526

On March 2, 2017 I discovered that my laptop computer which had been in the trunk of my car was missing upon arrival at my destination. The personal information that was stored on the laptop in a scanned copy of your long-term care insurance application included your name, address and phone number, [insert variable information]. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / NY AG's office Author:
Article Title: ACSIA Partners
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280499.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-26	Alignstaffing and RehabPlus Staffing Group	MD	3/30/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 16, 2017, Alignstaffing and RehabPlus Staffing Group, Inc. (collectively, the "Company") were the target of an email phishing scam that resulted in the unauthorized disclosure of some of our 2016 employees' private information. Specifically, 2016 W-2 tax information for some Company employees was released, including their names, social security numbers and compensation amounts, for current and former employees who received compensation from the Company during 2016.

Attribution 1 Publication: MD AG's office Author:
Article Title: Alignstaffing and RehabPlus Staffing Group
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280505.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-25	William E. Howe & Co., CPAs	PA	3/30/2017	Electronic	Business	Yes - Published #	1,831

A third-party data forensic firm was retained to assist in our investigation. While the investigation is ongoing, we have discovered unauthorized access to a tax program utilized by our company. The tax program stored the following categories: name, address, Social Security number, dates of birth, and in some cases, bank account information. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office / ME AG's office / NY AG Author:
Article Title: William E. Howe & Co., CPAs
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280494.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-24	Leavell Investment Management	AL	3/22/2017	Electronic	Business	Yes - Unknown #	Unknown

On December 19, 2016, a Leavell employee received a spoofed email appearing to be from one of our commonly used vendors that included a malicious link within the body ofthe email.

Attribution 1 Publication: MD AG's office Author:
Article Title: Leavell Investment Management
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281024.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-23	Contact Fill, LLC	PA	3/30/2017	Electronic	Business	Yes - Published #	125

Contact Fill was alerted by its website hosting company that our website had been taken off line and in response we worked with our hosting company to determine the root cause and what was needed to restore the website. As part of these efforts, the hosting company discovered malware on the website that appeared to be collecting credit card transactions that were keyed into the website between December 13, 2016 and December 21, 2016. (Exposure number per NY AG's office)

Attribution 1
Publication: MD AG's office / NY AG's office Author:
Article Title: Contact Fill, LLC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280496.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-22	Huckstep Holdings Corp. d/b/a TechWise	CO	3/3/2017	Electronic	Business	Yes - Unknown #	Unknown

On January 24, 2017, Form W-2 Wage and Tax Statement information for certain current and former employees of TechWise was disclosed in error.

Attribution 1
Publication: MD AG's office Author:
Article Title: Huskstep Holdings Corp. d/b/a TechWise
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280439%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-21	Bluestein, Michael & Company, PC	PA	3/31/2017	Electronic	Business	Yes - Published #	596

On January 28, 2017, Bluestein Michael discovered that its network had been affected by a ransomware program that encrypted certain files within our network. The information related to you that may have been subject to unauthorized access includes your name, address, <<bank account information >> and Social Security number. (Exposure number per NY AG's office)

Attribution 1
Publication: MD AG's office / NY AG's office Author:
Article Title: Bluestein, Michael & Company, PC
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280512.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-20	Lincoln Savings Bank	IA	3/31/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On or about February 2, 2017, we learned that a Lincoln employee sent, without having a job related reason to do so, an electronic document to his personal e-mail account on January 4, 2017 which contained information regarding certain Lincoln customers' accounts.

Attribution 1
Publication: MD AG's office Author:
Article Title: Lincoln Savings Bank
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280513.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-19	Offit Kurman Attorneys at Law	MD	3/31/2017	Electronic	Business	Yes - Unknown #	Unknown

At the conclusion of this representation, we prepared a package to return materials, including a thumb drive and a transmittal letter contain sensitive personal information. On February 29, 2016, we sent the package via U.S. mail. On On April 5, 2016, the package was returned to Offit Kurman after being damaged in transit. Based on our investigation, we believe that the data on the thumb drive may have included personal information related to you, including your name, Social Security number, driver's license number, tax ID number, and/or financial information.

Attribution 1
Publication: MD AG's office Author:
Article Title: Offit Kurman Attorneys at Law
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280526.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-18	Sophrona Solutions, Inc.	MN	3/31/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 23, 2017, we received a notification from a company in a foreign country that one of our servers had possibly been involved in an unauthorized attempt to access their servers. The personal information located in the files on the server included first names, last names, social security numbers, and, in some instances, dates of birth.

Attribution 1 Publication: MD AG's office Author:
Article Title: Sophrona Solutions, Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280507.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-17	Mary T. Inc.	MN	3/31/2017	Electronic	Business	Yes - Unknown #	Unknown

On or around January 24, 2017, a former MTI payroll administrator received a spoofed email requesting PDF copies of the 2016 W2s for current and former employees of MTI.

Attribution 1 Publication: MD AG's office Author:
Article Title: Mary T. Inc.
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280994.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-16	George Fox University	OR	4/21/2017	Electronic	Educational	Yes - Published #	1,774

An individual gained unauthorized access to a portion of the university's W-2 tax forms for the 2016 tax year, specifically affecting employees who did not select the electronic W-2 consent option. (Exposure number per NY AG's office)

Attribution 1 Publication: OR AG's office / MT AG's office / NY AG Author:
Article Title: George Fox University
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/944219645

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-15	Wild, Maney & Resnick	NY	4/21/2017	Electronic	Business	Yes - Published #	5,261

On March 8, 2017, Wild, Maney & Resnick, LLP ("WMR"), suspected that an unknown, unauthorized third-party may have accessed clients' tax information stored within our tax preparation software. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office / NY AG' Author:
Article Title: Wild, Maney & Resnick
Article URL: https://dojmt.gov/wp-content/uploads/Wild-Maney-Resnick.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-14	University of California / California Clinical Trials, LLC	CA	4/20/2017	Electronic	Educational	Yes - Unknown #	Unknown

The University of California today (April 20) announced it has uncovered a massive scheme targeting students through its student health plan that fraudulently obtained student information and then stole almost $12 million from UC by writing phony medical prescriptions in the students' names.

Attribution 1 Publication: University of California website Author:
Article Title: UC moves to shut down alleged fraud targeting students
Article URL: https://www.universityofcalifornia.edu/press-room/uc-moves-shut-down-alleged-fraud-targeting-students

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-13	**Blowout Cards**	VA	4/24/2017	Electronic	Business	Yes - Published #	**182**

Recently we were alerted to a potential security breach on our website. After researching this issue, our internet security team detected and patched an exploit that allowed unauthorized access to customers' card information when checking out on Blowoutcards.com. (Exposure per NY AG's office per notification from Discover)

Attribution 1 Publication: databreaches.net / NY AG's office Author:
Article Title: Blowout Cards Starts Notifying Customers After Card Fraud Reports Roll In
Article URL: https://www.databreaches.net/blowout-cards-starts-notifying-customers-after-card-fraud-reports-roll-in/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-12	**Valley Women's Health, S.C.**	IL	4/19/2017	Electronic	Medical/Healthcare	Yes - Published #	**5,155**

Valley Women's Health, S.C. IL Healthcare Provider 5155 04/19/2017 Hacking/IT Incident Electronic Medical Record, Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Valley Women's Health, S.C.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=0B8C6783EA55E240C1DC539928353A9A

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-11	**University of Oklahoma - OU Physicians**	OK	4/4/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,637**

University of Oklahoma, OU Physicians OK Healthcare Provider 1637 04/04/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=0B8C6783EA55E240C1DC539928353A9A
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=0B8C6783EA55E240C1DC539928353A9A

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-10	**MVP Health Care**	NY	4/14/2017	Electronic	Medical/Healthcare	Yes - Published #	**951**

MVP Health Care, Inc. NY Health Plan 951 04/14/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: MVP Health Care
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=0B8C6783EA55E240C1DC539928353A9A

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-09	**Carson Valley Medical Center**	NV	4/4/2017	Electronic	Medical/Healthcare	Yes - Published #	**11,368**

Carson Valley Medical Center NV Healthcare Provider 11368 04/04/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Carson Valley Medical Center
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=0B8C6783EA55E240C1DC539928353A9A

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-08	**BioReference Laboratories**	NJ	4/21/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,722**

An employee of New Jersey-based BioReference Laboratories has been terminated for failing to follow company protocols – and HIPAA Rules – regarding the secure disposal of documents containing the protected health information of patients. Company policies require all sensitive paperwork to be securely shredded prior to disposal, in accordance with HIPAA Rules. However, on March 14, 2017, BioReference Laboratories discovered that documents provided to the employee had been disposed of in a dumpster in Davenport, Florida.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Employee Terminated for Improperly Dumping PHI
Article URL: http://www.hipaajournal.com/employee-terminated-improperly-dumping-phi-8775/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-07	Cardiology Center of Acadiana	LA	4/21/2017	Electronic	Government/Military	Yes - Published #	9,681

A recent Cardiology Center of Acadiana ransomware attack has resulted in the exposure of almost 9,700 patients' protected health information. The ransomware attack occurred on February 7, 2017 and was discovered the following day. The attackers targeted a server used by the Lafayette, LA-based cardiology practice and deployed ransomware, which encrypted a range of files containing patients' names, dates of birth, addresses, billing information, clinical data, medical images and social security numbers.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Cardiology Center of Acadiana Ransomware Attack Impacts 9,700 Patients
Article URL: http://www.hipaajournal.com/cardiology-center-of-acadiana-ransomware-attack-impacts-9700-patients-8776/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-06	Campbell Union High School District	CA	4/20/2017	Electronic	Educational	Yes - Published #	3,232

During Spring Break there was unauthorized access into the District's electronic data systems. This unauthorized access may have involved some employee personal information, specifically employee Social Security numbers and addresses. I am writing to provide you information on the steps we are taking to protect you and your information moving forward. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NY AG's office Author:
Article Title: Campbell Union High School District
Article URL: https://oag.ca.gov/system/files/CUHSD%20Sample%20Letter_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-05	Northrop Grumman / Talx	VA	4/18/2017	Electronic	Business	Yes - Unknown #	Unknown

Equifax Workforce Solutions (aka TALX), our W-2 online portal provider, recently confirmed that an unauthorized third party(ies) gained access to its portal during various time periods from April 18, 2016 through March 29, 2017, and may have accessed your personal information and downloaded a copy of your 2016 W-2 form.

Attribution 1 Publication: CA AG's office Author:
Article Title: Northrop Grumman
Article URL: https://oag.ca.gov/system/files/Northrop%20Grumman%20Individual%20Notification%20Letter_64772036_1_0.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-04	Atlantic Digestive Specialists	NH	4/21/2017	Electronic	Medical/Healthcare	Yes - Published #	2,081

On February 20, 2017, ADS discovered that some of our systems were infected with ransomware. Our investigation revealed that the ransomware began affecting these systems on or around February 18, 2017. However, the systems that were impacted by this incident may have contained information including names, dates of birth, address information, telephone numbers, medical record numbers, health insurance information, and clinical/diagnostic information at the time of the incident.

Attribution 1 Publication: ADS website / hipaajournal.com / NH A Author:
Article Title: Atlantic Digestive Specialists, Notice of Data Breach
Article URL: http://atlanticdigestive.com/notice-data-privacy-event/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-03	Iowa Veterans Home	IA	4/21/2017	Electronic	Government/Military	Yes - Published #	2,969

According to a release from the IVH, Google and the state of Iowa were targeted with multiple phishing email campaigns in February and three IVH employees provided their credentials, which gave the hacker access to email accounts.

Attribution 1 Publication: kcrg.com Author:
Article Title: Iowa Veterans Home warns nearly 3,000 of data breach
Article URL: http://www.kcrg.com/content/news/Iowa-Veterans-Home-warns-nearly-3000-of-data-breach-420138664.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-02	Lifespan	RI	4/23/2017	Electronic	Medical/Healthcare	Yes - Published #	20,431

The hospital network says the computer was stolen from a car on Feb. 25. The laptop may have had work emails containing information about patients and their medication prescriptions, but it didn't have Social Security numbers, medical diagnoses and other sensitive information in the network's database.

Attribution 1 Publication: washingtontimes.com / hipaajournal.com Author:
Article Title: Lifespan notifies patients of potential data breach
Article URL: http://www.washingtontimes.com/news/2017/apr/23/lifespan-notifies-patients-of-potential-data-breac/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170424-01	J Bauer CPA, PLCC	AR	2/9/2017	Electronic	Business	Yes - Unknown #	Unknown

While we have no proof, we are handling these unusually high rejects as a possible past data breach of our data system. At this time, the extent of any possible data breach, to us, is unknown. We advise you to take appropriate precautions. If there was a breach, your social security number and other information could have been compromised.

Attribution 1 Publication: AR AG's office Author:
Article Title: J Bauer CPA, PLCC
Article URL: Per FOIA request AR AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170420-09	Schoolzilla	CA	4/20/2017	Electronic	Business	Yes - Published #	1,300,000

A student data warehouse platform, Schoolzilla first acknowledged the breach on April 12 in a message on its website, which informed customers: "A well-known computer security researcher was doing a targeted analysis of Schoolzilla when he uncovered a file configuration error."

Attribution 1 Publication: dailydot.com Author:
Article Title: 1.3 million K-12 students exposed by now-secured data breach
Article URL: https://www.dailydot.com/layer8/1-3-million-american-students-exposed-data-breach-now-secured/

Attribution 2 Publication: paloaltoonline.com Author:
Article Title: PAUSD student data exposed in breach
Article URL: https://www.paloaltoonline.com/news/2017/04/20/pausd-student-data-exposed-in-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170420-08	prAna	CA	3/8/2017	Electronic	Business	Yes - Published #	391,484

On February 6, 2017, we detected that an unauthorized third party may have obtained access to the servers that operate our e-commerce website, www.prana.com. The information that may have been affected includes your name, address, phone number, email address, payment card number ending in <<last 4 digits>>, expiration date and security code (CVV), and username and account password for our website. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / CA AG's office / SC AG' Author:
Article Title: prAna
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/prAna-20170308.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170420-07	Dixon Hughes Goodman LLP	NC	1/20/2017	Electronic	Business	Yes - Published #	1,500

On November I, 2016, we discovered an unknown individual had accessed the accountant's email account. While our investigation is ongoing, we determined on December 30, 2016, after a lengthy programmatic and manual review of the contents of the email account, that the following information relating to you was contained in the email account at the time of this incident: Social Security number, Driver's License number, financial account number, and name. (Exposure number per NY AG's office)

Attribution 1 Publication: SC AG's office / NY AG's office Author:
Article Title: Dixon Hughes Goodman LLP
Article URL: Per FOIA request SC and FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170420-06	Saint-Gobain Corporation / Talx	PA	4/13/2017	Electronic	Business	Yes - Unknown #	Unknown

In March 2017, SGC discovered that at various times between approximately April 2016 and March 2017, a third party accessed a MyPay system hosted and serviced by SGC's third-party service provider, Talx Corporation, a wholly-owned subsidiary of Equifax Inc. ("Talx"). Upon accessing accounts, the unauthorized party was able to
view pay stubs, pay histories, and W-4 and W-2 forms. SGC is not aware of any other information that was accessed.

Attribution 1 Publication: Nh AG's office Author:
Article Title: Saint-Gobain Corporation
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/saint-gobain-20170413.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170420-05	Forest City Trading Group	OR	4/3/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 1, 2017, we learned that equipment was stolen. Among the items stolen was a laptop that contained some information related to the employee stock ownership plan ("ESOP").

Attribution 1 Publication: NH AG's office Author:
Article Title: Forest City Trading Group
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/forest-city-trading-20170403.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170420-04	Citizens Financial Group (4/4/17)	RI	4/5/2017	Electronic	Banking/Credit/Financial	Yes - Published #	461

The skimming events took place on various dates in February 2017, and were discovered by Citizens on March 22, 2017. Customer name, debit card number, and PIN were compromised as a result of this incident. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Citizens Financial Group (4/4/17)
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/citizens-20170405.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170420-03	Citizens Financial Group (4/13)	RI	4/13/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

The skimming events took place on various dates in January 2017, and were discovered by Citizens on April 10, 2017. Customer name, debit card number, and PIN were compromised as a result of this incident.

Attribution 1 Publication: NH AG's office Author:
Article Title: Citizens Financial Group (4/13)
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/citizens-20170413.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170420-02	**Pacific Lutheran University**	WA	4/18/2017	Electronic	Educational	Yes - Published #	**955**

On January 26, 2017, PLU became aware of a “phishing” email sent to certain PLU staff and student email accounts on January 23, 2017. That email was fraudulently written to appear as if it was sent by university President, Thomas Krise, and prompted recipients to enter their PLU email account username and password. Our investigation determined the following types of your information were stored within one or more affected email accounts: name, <<ClientDef1 (driver’s license number, state identification card number, Social Security number, financial account information, payment card number, student identification number, transcript, medical information, health insurance information, username/password, passport number, date of birth)>>.

Attribution 1 Publication: MT AG's office / CT AG's office / NY AG Author:
Article Title: Pacific Lutheran University
Article URL: https://dojmt.gov/wp-content/uploads/Pacific-Lutheran-University.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170420-01	**Another Broken Egg Café**	SC	4/19/2017	Electronic	Business	Yes - Unknown #	**Unknown**

A Mount Pleasant breakfast restaurant says hackers may have gotten a hold of its diners' credit card numbers earlier this year. Another Broken Egg Cafe says the card processing systems in some of its locations were breached in late January, and criminals might have collected credit card information over the next two months.

Attribution 1 Publication: postandcourier.com Author:
Article Title: Mount Pleasant restaurant Another Broken Egg Cafe says hackers may have gotten diners' credit card numbers
Article URL: http://www.postandcourier.com/business/mt-pleasant-restaurant-another-broken-egg-cafe-hit-by-data/article_a0386aa

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170418-01	**Payless Décor LLC**	GA	4/10/2017	Electronic	Business	Yes - Unknown #	**Unknown**

From March 31, 2016, through December 9, 2016, there was illegal and unauthorized access to customer account information. An unauthorized individual may have used the Internet to gain access to customer payment card data.

Attribution 1 Publication: WI AG's office Author:
Article Title: Payless Décor LLC
Article URL: https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-12	**Dutchland Plastics**	WI	2/2/2017	Electronic	Business	Yes - Published #	**424**

On Thursday, February 2, 2017 Dutchland Plastics discovered that it was the victim of a phishing cyber-scam which resulted in a data breach. As a result of the phishing scam, the personal information of current and former employees of Dutchland Plastics, who received a W-2 for 2017, was compromised.

Attribution 1 Publication: WI AG's office Author:
Article Title: Dutchland Plastics
Article URL: https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-11	**Dental Services Group / Sentage Corporation**	MN	2/1/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

On January 30, 2017 an individual fraudulently posing as the CEO of Dental Services Group requested the 2016 W-2 forms of employees. The phishing scam resulted in the inadvertent disclosure of employee personal information, including names, addresses, Social Security numbers, wages and tax information.

Attribution 1 Publication: WI AG's office / AR AG's office Author:
Article Title: Dental Services Group / Sentage Corporation
Article URL: https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-10	**Amedisys Home Health of Fayetteville / Amedisys West**	NC	4/16/2017	Paper Data	Medical/Healthcare	Yes - Published #	**611**

Amedisys Home Health of Fayetteville was recently informed that two bins used for collecting shredded materials from the Fayetteville care center were found in an enclosure behind a local business, and did not reach the vendor's intended destination to a secure shredding facility

Attribution 1 Publication: montgomery-herald.com / hipaajournal.c Author:
Article Title: Amedisys announces patient info breach
Article URL: http://www.montgomery-herald.com/news/amedisys-announces-patient-info-breach/article_4180ef04-224e-11e7-9dfe-4

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-09	**Johnson, Hearn, Vinegar & Gee**	NC	4/14/2017	Electronic	Business	Yes - Published #	**7,958**

On January 16,2017, we became aware of a ransomware attack of our computer system. Ransomware is used by an Internet-based attacker to remotely lock the victim's computer system. The attacker then demands that a ransom be paid to remove the restriction. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office / CT AG' Author:
Article Title: Johnson, Hearn, Vinegar & Gee
Article URL: https://dojmt.gov/wp-content/uploads/Johnson-Hearn-Viinegar-Gee.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-08	**Combat Brands, LLC**	KS	4/14/2017	Electronic	Business	Yes - Published #	**37,863**

On January 25, 2017, we began investigating some unusual activity reported by our credit card processor. We immediately began to work with third-party forensic experts to investigate these reports and to identify any signs of compromise on our systems. (Exposure number per NY AG's office per notification from Discover)

Attribution 1 Publication: MT AG's office/ CA AG's office / OR AG' Author:
Article Title: Combat Brands, LLC
Article URL: https://dojmt.gov/wp-content/uploads/Combat-Brands.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-07	**FPI Management, Inc.**	CA	4/10/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Between January 19 and 27, 2017, we mailed out Form 1099s to our contractors. On or around January 31, 2017, we learned that in the process of preparing the Form 1099s for mailing, some were inadvertently placed in the wrong envelopes.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-06	**One World Distribution, Inc. / Gildan**	SD	4/7/2017	Electronic	Business	Yes - Published #	**7,552**

One World Distribution, Inc. d/b/a One World Direct ("OWD") is writing regarding a recent data security incident that may impact certain payment card and demographic information used by you at the e-commerce website, www.gildanonline.com, between August 27, 2016, and February 15, 2017. OWD is providing this notice on behalf of Gildan because OWD hosts and operates gildanonline.com (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office / ME AG Author:
Article Title: One World Distribution, Inc.
Article URL: https://dojmt.gov/wp-content/uploads/One-World-Distribution.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-05	Best American Hospitality Corp. / Shoney's	TN	4/17/2017	Electronic	Business	Yes - Unknown #	Unknown

Multiple sources in the financial industry say they've traced a pattern of fraud on customer cards indicating that the latest victim may be Shoney's, a 70-year-old restaurant chain that operates primarily in the southern United States.

Attribution 1 Publication: krebsonsecurity.com Author:
Article Title: Shoney's Hit By Apparent Credit Card Breach
Article URL: https://krebsonsecurity.com/2017/04/shoneys-hit-by-apparent-credit-card-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-04	Westminster College	MO	4/16/2017	Electronic	Educational	Yes - Published #	Unknown

The breach of employee information was discovered March 26, according to a statement from Lana Poole, vice president and chief communications officer at Westminster. Poole said the breach was the result of a phishing scam and was reported to law enforcement authorities.

Attribution 1 Publication: columbiatribune.com Author:
Article Title: Westminster College reports employee data breach
Article URL: http://www.columbiatribune.com/import/westminster-college-reports-employee-data-breach/article_a3508d34-af9e-507

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-03	Unified Health Infrastructure Project (UHIP) / RI Office of	RI	4/14/2017	Electronic	Government/Military	Yes - Published #	5,600

A file containing embedded personal information for an estimated 5,600 Rhode Island benefit recipients was recently discovered on the state's Transparency Portal and its General Assembly websites, according to a statement the Rhode Island Office of Health & Human Services released yesterday.

Attribution 1 Publication: Becker's Health IT & CIO Review Author:
Article Title: Rhode Island state benefits system potentially exposes 5.6k recipients
Article URL: Rhode Island state benefits system potentially exposes 5.6k recipients

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-02	DLD Accountancy, LLP	CA	3/3/2017	Electronic	Business	Yes - Published #	818

On or about March 20, 2017, DLD Accountancy, LLP became aware that it was the victim of a cyberattack by which an unknown third party was able to access DLD Accountancy, LLP 's computer network and some of its clients' personal information. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office NY AG's office Author:
Article Title: DLD Accountancy, LLP
Article URL: https://oag.ca.gov/system/files/Sample%20Consumer%20Notification%20letter%20Non-CT%20%28110082750_1%29_0.

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170417-01	Virginia Mason Memorial	WA	4/17/2017	Electronic	Medical/Healthcare	Yes - Published #	419

Audits of PHI access logs occasionally reveal rogue employees have been improperly accessing the medical records of patients, but what makes this incident stand out is the number of employees that were discovered to have improperly viewed PHI. The types of information accessed includes demographic information and patients' medical records. In some instances, it is possible that Social Security numbers were viewed, although financial information was not accessed by any of the employees.

Attribution 1 Publication: hipaajournal.com / Yakima Herald Author:
Article Title: 21 Employees Found to Have Accessed PHI Without Authorization
Article URL: http://www.hipaajournal.com/21-employees-found-to-have-accessed-phi-without-authorization-8770/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170414-06	**BankSouth Mortgage**	GA	4/11/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	**Unknown**

On February 7, 2017, we discovered that the email accounts of two BankSouth Mortgage employees were accessed without authorization on February 3, 2017. The information that may have been involved includes names, addresses, dates of birth, Social Security numbers, driver's license numbers and credit card numbers.

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: BankSouth Mortgage
Article URL: https://dojmt.gov/wp-content/uploads/BankSouth-Mortgage.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170414-05	**Tidewater Transit Company, Inc.**	NC	4/13/2017	Electronic	Business	Yes - Unknown #	**Unknown**

In late March 2017 we learned that certain of our employees had been the targets of tax-related identity theft. We do know that some of our employees who were targets of tax-related identity theft were also notified by the IRS that their tax information may have been unlawfully obtained from the IRS through the data retrieval tool available from the U.S. Department of Education Free Application for Student Financial Aid

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170414-04	**Bluestem Brands, Inc. / Fingerhut / Gettington**	MN	4/7/2017	Electronic	Business	Yes - Published #	**10,897**

We believe that your personal information was accessed by cyber-attackers executing an attempt to obtain unauthorized access to your Fingerhut account between March 24, 2017 and April 7, 2017.
The account data accessed may have included personal information such as your name and address, email address, phone number, and credit account number. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NH AG' Author:
Article Title: Bluestem Brands, Inc. / Fingerhut
Article URL: https://oag.ca.gov/system/files/72494_California_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170414-03	**Alamo Capital Financial Services**	CA	3/14/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**1,537**

On March 14, 2017, a data security incident occurred which may have affected your personal information. The incident may have involved names, dates of birth, and Social Security numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NY AG' Author:
Article Title: Alamo Capital
Article URL: https://oag.ca.gov/system/files/Alamo%20Capital%20-%20consumer%20notification%20letter%20-%2004132017_0.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170414-02	**Delta Career Education Corporation**	VA	2/13/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

On March 30, 2017, Delta Career completed an investigation regarding suspicious activity in its computer network The investigation recently determined that unauthorized persons may have accessed information relating to some of our current and former employees. The information potentially affected includes your name, address, and Social Security number.

Attribution 1 Publication: CA AG's office / Vt AG's office Author:
Article Title: Delta Career Education Corporation
Article URL: https://oag.ca.gov/system/files/Employee%20CA_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170414-01	Neiman Marcus Group	TX	4/14/2017	Electronic	Business	Yes - Published #	6,494

On or about January 17, 2017, unauthorized individuals began attempting to access our InCircle, Neiman Marcus, Bergdorf Goodman, Last Call, CUSP, and Horchow websites (collectively the "NMG websites") by trying various login and password combinations using automated attacks. The intruders were able to access customers' names, basic contact information, email addresses, purchase history, but only the last four digits of payment card numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / VT AG's office / MT AG' Author:
Article Title: Neiman Marcus
Article URL: https://oag.ca.gov/system/files/NMG-CA%20PCI-PII%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170413-04	River City Media	US	3/6/2017	Electronic	Business	Yes - Unknown #	Unknown

One of the largest spam operations in the world has exposed its entire operation to the public, leaking its database of 1.37bn email addresses thanks to a faulty backup.

Attribution 1 Publication: csoonline.com Author:
Article Title: SpammerGate: The takeaway lessons and follow-ups on the River City Media data breach
Article URL: http://www.csoonline.com/article/3178395/security/spammergate-the-takeaway-lessons-and-follow-ups-on-the-river-cit

Attribution 2 Publication: theguardian.com Author:
Article Title: Spam email operator's faulty backup leaks 1.37bn addresses
Article URL: https://www.theguardian.com/technology/2017/mar/06/email-addresses-spam-leak-river-city-media

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170413-03	TriTech Software Systems	CA	3/30/2017	Electronic	Business	Yes - Published #	863

We recently discovered that our company was the victim of an email spoofing attack on February 16, 2017, by an individual pretending to be our Chief Executive Officer. A request was made from what appeared to be a legitimate TriTech email address for all 2016TnTech employee W-2 information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / CT AG' Author:
Article Title: TriTech Software Systems
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/tritech-software-20170330.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170413-02	Bank of America	CA	2/21/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

An incident occurred on February 8, 2017 that may have resulted in the disclosure of your information due to an employee fax error. We have been unsuccessful in our attempts to request destruction of the documents. According to our records, the information involved in this incident was related to your loan and included your first and last name, address, Social Security number and employment information.

Attribution 1 Publication: TX AG's office Author:
Article Title: Bank of America
Article URL: Per FOIA request / TX AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170413-01	De Wafelbakkers	AR	2/24/2017	Electronic	Business	Yes - Unknown #	Unknown

Our client, De Wafelbakkers, suffered a data breach in which W2 forms for its current and former employees were sent to an unauthorized individual as a result of a spoofed email.

Attribution 1 Publication: TX AG's office / AK AG's office Author:
Article Title: De Wafelbakkers
Article URL: Per FOIA request / TX AG's office and AK AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170412-03	Children's Place / Ceridian	NJ	4/4/2017	Electronic	Business	Yes - Published #	135

We recently learned that an unauthorized party may have accessed certain employees' personal information on www.ereports.ceridian.com, a website hosted by Ceridian, our third-party payroll tax vendor. The personal information may have included data contained on W-2 tax forms, such as names, addresses, Social Security numbers, and wage and tax information. (Exposure number per NY AG's office)

Attribution 1 Publication: Nh AG's office / ME AG's office / NY AG' Author:
Article Title: Children's Place / Ceridian
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/childrens-place-20170404.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170412-02	Hospice of North Central Ohio	OH	3/23/2017	Electronic	Medical/Healthcare	Yes - Published #	1,051

Hospice of North Central Ohio OH Healthcare Provider 1051 03/23/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: Hospice of North Central 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
ITRC20170412-01	Women's Care of Somerset	KY	3/31/2017	Electronic	Medical/Healthcare	Yes - Published #	1,806

On February 3, 2017, Women's Care of Somerset (WCS) employees erroneously disclosed the email addresses of all recipients of an informative email regarding health-related services to the other recipients.

Attribution 1 Publication: hhs.gov / healthitsecurity.com Author:
Article Title: Kentucky Health Center Ensures PHI Security After Email Gaffe
Article URL: http://healthitsecurity.com/news/kentucky-health-center-ensures-phi-security-after-email-gaffe

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170411-01	HealthNow Networks	FL	4/10/2017	Electronic	Business	Yes - Published #	918,000

The data of 918,000 patients who provided their sensitive information to HealthNow Networks, a Boca Raton, FL-based telemarketing organization that used to provide medical supplies to seniors, has been exposed online for many months. The database contained a range of highly sensitive data including individuals' names, addresses, email addresses, telephone numbers, dates of birth, Social Security numbers, health insurance information and medical conditions.

Attribution 1 Publication: hippajournal.com Author:
Article Title: 918,000 Patients' Sensitive Information Exposed Online
Article URL: http://www.hipaajournal.com/918000-patients-sensitive-information-exposed-online-8762/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170410-04	Sarnova, Inc.	OH	3/31/2017	Electronic	Business	Yes - Published #	720

On March 1, 2017, we learned that some employees had fraudulent tax retmns filed. We immediately began an investigation, and determined that a targeted "spear phishing" email had been sent to a Sarnova employee on January 20, 2017. Spear phishing emails are an attempt to solicit personal information from unsuspecting users byappearing as if they had been sent from a legitimate organization or known individual. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / ME A Author:
Article Title: Sarnova, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/sarnova-20170331.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170410-03	Elbit Systems	NH	4/3/2017	Electronic	Business	Yes - Unknown #	Unknown

Our initial investigation indicates that the unauthorized access did not occur through our systems, but we are reporting this to you nevertheless.We have also been actively working with our third party vendors and have hired a third party security consultant to investigate our internal systems. To date, there has been no indication that any compromise occurred within our internal systems or with our third party vendors. Since we have no evidence that an intrusion occurred in our systems, we cannot be more precise as to thedate fraudulent information started being used within the IRS nor the specific types of infonnation that is being misused.

Attribution 1 Publication: NH AG's office / ME AG's office / NY AG Author:
Article Title: Elbit Systems
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/elbit-systems-20170403.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170410-02	Envelopes Unlimited	MD	3/31/2017	Electronic	Business	Yes - Published #	542

On March 29, 2017, we learned that a targeted "spear phishing" email message had been sent to an Envelopes Unlimited employee earlier that day. The email the employee received was designed to appear though it had been sent to the employee by an Envelopes Unlimited executive, requesting 2016 Forms W2. Believing the email to be legitimate, the employee replied to the message and attached 2016 Forms W2, which included employees' names, addresses, Social Security numbers, and earnings information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Envelopes Unlimited
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/envelopes-unlimited-20170331.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170410-01	Solera Holding, Inc.	TX	3/31/2017	Electronic	Business	Yes - Published #	4,832

We recently learned that a data compromise may have occurred at a Solera company or at an outside vendor to a Solera company. Since then, we have been and are continuing to investigate the suspected data compromise to determine its source and effect any required remediation measures. (Exposure number per NY AG's office)

Attribution 1 Publication: OR AG's office / NH AG's office / VT AG' Author:
Article Title: Solera Holding, Inc.
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1066549897

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170407-05	Gamestop	TX	4/7/2017	Electronic	Business	Yes - Published #	1,338,102

GameStop recently received notification from a third party that it believed payment card data from cards used on the GameStop.com website was being offered for sale on a website," a company spokesman wrote in response to questions from this author. (Exposure number per NY AG's office)

Attribution 1 Publication: krebsonsecurity.com / WI AG's office / C Author:
Article Title: Gamestop.com Investigating Possible Breach
Article URL: https://krebsonsecurity.com/2017/04/gamestop-com-investigating-possible-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170407-04	Carlson Rezidor Hotel Group	MN	4/4/2017	Electronic	Business	Yes - Unknown #	Unknown

On [Date], we discovered that your guest reservation data, which had previously been provided to a Carlson Rezidor employee, may have been acquired in a manner that may have compromised your personal information. The information involved may have included your name, address, and credit card information, including the security code.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170407-03	Brophy Dailey & Incardona, LLP	NY	4/5/2017	Electronic	Business	Yes - Published #	831

In early February, we began receiving reports from a handful of clients about letters they received from the IRS seeking to confirm that they had electronically filed their return for 2016 when they had not. Upon learning of these letters, we immediately engaged computer experts to investigate if our systems were at risk. Although the investigation has identified no evidence of unauthorized access to your information, it is possible that your name, address, Social Security number and tax information were obtained by an unauthorized individual. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NY AG's office Author:
Article Title: Brophy Dailey & Incardona, LLP
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Brophy%20Dailey%20&%20Incardona%20LL%20SBN%

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170407-02	Skin Cancer Specialists, PC	GA	4/7/2017	Electronic	Medical/Healthcare	Yes - Published #	3,365

Atlanta-based Skin Cancer Specialists, P.C., has announced a data security incident has been discovered that has resulted in the exposure of the billing records of 3,365 patients. An unauthorized individual was discovered to have gained access to the healthcare provider's system on October 15, 2016, with the intrusion detected on February 2, 2017.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: 3,365 Patients' Billing Records Potentially Stolen by Hacker
Article URL: http://www.hipaajournal.com/3365-patients-billing-records-potentially-stolen-by-hacker-8760/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170407-01	IRS - Data Retrieval Tool	DC	4/6/2017	Electronic	Government/Military	Yes - Published #	100,000

Internal Revenue Service Commissioner John Koskinen said Thursday the information of up to 100,000 taxpayers may have been stolen in a security breach of an online tool used to apply for federal student aid.

Attribution 1 Publication: sltoday.com Author:
Article Title: Identity thieves may have hacked files of 100,000 FAFSA applicants
Article URL: http://www.stltoday.com/news/local/crime-and-courts/identity-thieves-may-have-hacked-files-of-fafsa-applicants/articl

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170406-07	Cincinnati Eye Institute	OH	3/14/2017	Electronic	Medical/Healthcare	Yes - Published #	500

Cincinnati's largest chain of eye surgeons may have been hit with a data breach, according to employees who tell 9 On You Side they have been unable to file their taxes. CEI Vice President of Marketing Don Holmes tells 9 On Your Side that employee information may have been accessed through an outside vendor, such as a company that handles payroll or benefits.

Attribution 1 Publication: wcpo.com Author:
Article Title: Possible data breach at Cincinnati Eye Institute
Article URL: http://www.wcpo.com/money/consumer/dont-waste-your-money/cincinnati-eye-institute-possible-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170406-06	Edgar & Associates, LLP	CA	4/6/2017	Electronic	Business	Yes - Published #	3,803

On March 13, 2017, a specialized forensic IT firm determined that hackers had gained unauthorized access to our system from a foreign IP address. If you are an individual, this information may have included your: name, date of birth, telephone number(s), address, Social Security number, all employment (W-2) information, 1099 information (including account number if provided to us), direct deposit bank account information (including account number and routing information if provided to us).

Attribution 1 Publication: CA AG's office / NY A's office Author:
Article Title: Edgar & Associates, LLP
Article URL: https://oag.ca.gov/system/files/Edgar%202_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170406-05	**University of Louisville / Talx**	KY	4/5/2017	Electronic	Educational	Yes - Published #	**850**

750 U of L employees were notified of suspicious activity on their tax returns via email April 4. Employee accounts showing suspicious activity have risen to 850, TALX reports.

Attribution 1 Publication: louisvillecardinal.com Author:
Article Title: Updated: Hackers steal university employee tax info
Article URL: http://www.louisvillecardinal.com/2017/04/hackers-steal-university-employee-tax-info/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170406-04	**Memorial Healthcare**	MI	4/3/2017	Electronic	Medical/Healthcare	Yes - Published #	**685**

Memorial Healthcare MI Healthcare Provider 685 04/03/2017 Unauthorized Access/Disclosure Other

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170406-03	**Ashland Women's Health**	KY	4/4/2017	Electronic	Medical/Healthcare	Yes - Published #	**19,727**

Ashland Women's Health KY Healthcare Provider 19727 04/04/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov / healthcareinfosecurity.com Author:
Article Title: Another Ransomware Attack Added to HHS Breach Tally
Article URL: http://www.healthcareinfosecurity.com/another-ransomware-attack-added-to-hhs-breach-tally-a-9825?rf=2017-04-12_E

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170406-02	**C. Kirk Holt & Associates**	UT	4/4/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On March 20, 2017, the specialized forensic IT firm hired to investigate this matter determined that an unauthorized person gained access to our system, and identification of what information may be impacted was begun.

Attribution 1 Publication: MT AG's office Author:
Article Title: C. Kirk Holt & Associates
Article URL: https://dojmt.gov/wp-content/uploads/C-Kirk-Holt-Associates.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170406-01	**Scottrade Bank / Genpact**	MO	4/6/2017	Electronic	Banking/Credit/Financial	Yes - Published #	**8,517**

Scottrade Bank recently acknowledged that an unsecured MSSQL database managed by a third-party vendor had exposed at least 20,000 customers' sensitive data, Salted Hash reports. (Genpact) (Exposure number per NY AG's office)

Attribution 1 Publication: NY AG's office / CA AG's office / MT AG' Author:
Article Title: Genpact
Article URL: Per FOIL NY AG's office

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170405-04	**Total Phase**	CA	3/24/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On March 16, 2017, Total Phase discovered that it had been the victim of a cyber attack. Cyber attackers installed unauthorized code on our website to harvest information from customers' web browsers during the checkout process.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Total Phase
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/total-phase-20170324.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170405-03	Spaulding Youth Center	NH	3/31/2017	Electronic	Business	Yes - Unknown #	Unknown

On Monday, March 20, 2017, we were notified by a staff member that she had experienced a problem with filing her tax return with the Internal Revenue Service because an unauthorized person had already filed a return linked to her personal information. We have subsequently determined that an unknown source obtained access to some employees' W2 information, including names, addresses, social security numbers, and other information. Based on our investigation, the theft of personal information occurred on February 6, 2017.

Attribution 1 Publication: NH AG's office / CT AG's office Author:
Article Title: Spaulding Youth Center
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/spaulding-youth-center-20170331.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170405-02	Behavioral Health Center	ME	4/5/2017	Electronic	Medical/Healthcare	Yes - Published #	4,229

In what may be the worst breach of 2017 so far in terms of highly sensitive and confidential patient records, a behavioral and mental health center in Maine recently learned that its patients' records – including evaluations, session notes, and records of sex offenders and sex abuse victims – had not only been in the hands of one criminal, but had reportedly been sold to an unknown party for unknown purposes.

Attribution 1 Publication: databreaches.net / bangordailynews.co Author:
Article Title: Highly confidential psychotherapy records from Maine center listed on the dark web
Article URL: https://www.databreaches.net/highly-confidential-psychotherapy-records-from-maine-center-listed-on-the-dark-web/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170404-06	North Carolina Department of Motor Vehicles	NC	4/4/2017	Electronic	Government/Military	Yes - Published #	24,000

The improper document disposal included records collected between Sept. 1, 2016 and March 7, 2017, according to the DMV's notice. The forms included in the boxes included insurance verification, driver current history detail and voter registration, which contained names, addresses, dates of birth and social security numbers.

Attribution 1 Publication: statescoop.com Author:
Article Title: North Carolina data breaches expose internal documents, personal records
Article URL: http://statescoop.com/2-north-carolina-data-breaches-expose-internal-documents-personal-records

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170404-05	Language Services Associates, Inc.	PA	3/27/2017	Electronic	Business	Yes - Published #	1,475

On February 10, 2017, LSA became aware of unauthorized access to its Human Resources Director's email account after that email account was used by an unknown actor to send out malicious "phishing" emails to LSA employees and other individuals on that same date. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / NY AG Author:
Article Title: Language Services Associates, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/language-service-associates-20170327.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170404-03	ABCD Pediatrics, PA	TX	3/26/2017	Electronic	Medical/Healthcare	Yes - Published #	55,447

San Antonio, TX-based ABCD Pediatrics has discovered cybercriminals gained access to its servers and encrypted data with ransomware, including the protected health information of its patients. The individuals behind the attack may also have gained access to data stored on the healthcare provider's servers prior to ransomware being deployed.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: More than 55,000 Patients Impacted by ABCD Pediatrics Ransomware Attack
Article URL: http://www.hipaajournal.com/more-than-55000-patients-impacted-by-abcd-pediatrics-ransomware-attack-8753/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170404-02	Apex EDI, Inc.	UT	3/31/2017	Electronic	Medical/Healthcare	Yes - Published #	1,132

Apex EDI, Inc. UT Business Associate 1132 03/31/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Apex EDI, 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
ITRC20170404-01	PenServ Plan Services / Security Finance	SC	3/31/2017	Electronic	Business	Yes - Unknown #	Unknown

In connection with its services as plan administrator, PenServ recently sent plan participants an email notifying them of their various plan options and benefits guides. Unfortunately, this email inadvertently included a spreadsheet containing plan participants' personal information to some of its recipients.

Attribution 1 Publication: MT AG's office / SC AG's office / CT AG' Author:
Article Title: PenServ Plan Services
Article URL: https://dojmt.gov/wp-content/uploads/PenServ-Plan-Services-Inc..pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170403-08	Veolia North America	MA	3/23/2017	Electronic	Business	Yes - Published #	684

On January 26, 2017, our third-party provider hosting the Server (the "Host) was notified of malicious activity on the Server by the attacker. This information may include your first and last name, company name, address, email address, usemame and password for your account on our website, and order history maintained on the website. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / NY AG Author:
Article Title: Veolia North America
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/veolia-north-america-20170323.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170403-07	Glenn R. Millar, CPA, PC	AZ	3/29/2017	Electronic	Business	Yes - Published #	1,313

Based on our investigation to date, we believe unauthorized persons hacked into our information systems between the period of May to July 2016, and used data on the system to fraudulently file federal income tax returns. The personal information that may have been acquired includes name, birth date, telephone number(s), address, social security number, financial account information, and bank account information including account number and routing information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: Glenn R. Millar, CPA, PC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/millar-cpa-20170329.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170403-06	Hotel Zelos / VHG Fourth Street SF, LLC	CA	3/28/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 26, 2017, we learned that a hotel laptop computer had been stolen that day from an internal office at Hotel Zelos. On the same day, we notified the police and filed a police report. Our investigation confirmed that the computer contained your name, address, payment card number, and expiration date.

Attribution 1 Publication: NH AG's office Author:
Article Title: Hotel Zelos / VHG Fourth Street SF, LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/hotel-zeloz-20170328.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170403-05	Great Falls Holdings, Inc.	ME	3/24/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 21, 2017, we learned that the 2016 W-2 Wage and Tax Statement Forms for company employees were apparently compromised as a result of a data breach that occurred on February 23, 2017. As a result, your personal information may have been exposed to third-parties who may try to misuse it to file a false tax return in your name, to open accounts in your name, or for other purposes. The information compromised consists of all information contained on your 2016 W-2 statement.

Attribution 1 Publication: NH AG's office / ME AG's office Author:
Article Title: Great Falls Holdings, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/great-falls-20170324.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170403-04	Christie's Inc.	NY	3/24/2017	Electronic	Business	Yes - Published #	428

Christie's recently discovered that it was victimized by a targeted e-mail phishing scam in which an unknown individual was able to obtain and use the e-mail log in credentials for three Christie's employees. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / NY AG Author:
Article Title: Christie's Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/christies-20170324.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170403-03	Krehbiel and Associates CPA	IL	3/30/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 27, 2017, a limited number of Krehbiel clients contacted us regarding notifications they had received from the IRS indicating possible fraudulent activity involving their accounts. On March 10, our forensics investigation determined that an unauthorized individual accessed our system between February 2 and February 13, 2017. These records include information used to prepare tax returns, including your name, address, Social Security number, wage information, and bank account information if you provided it to us.

Attribution 1 Publication: MT AG's office Author:
Article Title: Krehbiel and Associates CPA
Article URL: https://dojmt.gov/wp-content/uploads/Krehbiel-and-Associates-CPA.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170403-02	Maloney & Kennedy, PLLC	NH	3/29/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 15, 2017, Maloney & Kennedy, PLLC, became aware that some clients' tax returns had been filed by an unknown third party. It appears that the IRS did not process any of those returns.The investigation determined that information including your name, address and Social Security number and 2015 tax information may have been accessed by an unknown third party.

Attribution 1 Publication: MT AG's office / NH AG's office / ME AG Author:
Article Title: Maloney & Kennedy, PLLC
Article URL: https://dojmt.gov/wp-content/uploads/Maloney-Kennedy-PLLC.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170403-01	Ameriflight	TX	3/28/2017	Electronic	Business	Yes - Published #	876

The Company recently learned that during the week of March 20, 2017 an unauthorized person posed as an executive of the Company and sent an email to a number of employees requesting certain employment-related information. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170330-02	**ShowTix4U**	NV	2/2/2017	Electronic	Business	Yes - Published #	**27,833**

We were recently alerted by our payment card processor to a potential security incident involving our website. Based upon an ongoing forensic investigation, it appears that an unauthorized actor was able to gain access to our third-party vendor's server and install malicious software on our website. The malicious software appears designed to capture payment card information as the information was inputted. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NY AG's office Author:
Article Title: ShowTix4U
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_5.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170330-01	**Quench USA Inc.**	PA	2/10/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On February 13, 2017, we discovered our Coffee Service server had been infected with a virus that prohibited our access to our files.On February 22, 2017, as part of our ongoing investigation, we determined this virus was introduced by an unknown third party that had access to a server on our information system and confirmed this server contains information relating to Quench Coffee Service customers.

Attribution 1 Publication: CA AG's office Author:
Article Title: Quench USA Inc.
Article URL: https://oag.ca.gov/system/files/Quench%20--%20notice%20only%201%20--%20California_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170329-03	**WellSpan Health**	PA	3/23/2017	Paper Data	Medical/Healthcare	Yes - Published #	**732**

WellSpan Health PA Health Plan 732 03/23/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: WellSpan 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
ITRC20170329-02	**Mecklenburg County Health Department**	NC	3/29/2017	Electronic	Government/Military	Yes - Published #	**2,081**

A spreadsheet containing the protected health information of more than 1,200 patients has been accidentally sent to two media outlets by a worker at Mecklenburg County, NC. Update: County Manager Dena Diorio updated Commissioners Tuesday evening saying 2,081 patients were impacted when county staff mistakenly released that information to the media last week.

Attribution 1 Publication: hipaajournal.com / twcnews.com / hhs.g Author:
Article Title: Patients' PHI Accidentally Sent to Media Outlets by Mecklenburg County
Article URL: http://www.hipaajournal.com/patients-phi-sent-media-mecklenburg-county-8748/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170329-01	**Virginia Gift Brands / WoodWick**	OH	3/27/2017	Electronic	Business	Yes - Published #	**4,111**

On February 17, 2017, we began investigating unusual activity reported by our credit card processor. On February 28, 2017, we confirmed that our system had been compromised, potentially resulting in unauthorized access to debit and credit card information used on our site between August 18, 2016 and February 20, 2017. (Exposure number per NY AG's office / notification from Discover)

Attribution 1 Publication: MT AG's office / ME AG's office / NY AG Author:
Article Title: Virginia Gift Brands / WoodWick
Article URL: https://dojmt.gov/wp-content/uploads/Virginia-Gift-Brands.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-10	Specialty Dental Partners of Philadelphia, PLLC dba Rich	PA	3/23/2017	Electronic	Medical/Healthcare	Yes - Published #	960

Specialty Dental Partners of Philadelphia, PLLC.- DBA Rich Orthodontics PA Healthcare Provider 960 03/23/2017 Theft Desktop Computer, Laptop

Attribution 1 Publication: hhs.gov Author:
Article Title: Specialty Dental Partners of Philadelphia, PLLC dba Rich Orthodontics
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-09	Bowling Green State University	OH	3/24/2017	Electronic	Educational	Yes - Unknown #	Unknown

BGSU had planned later this summer to make 2FA mandatory for access to the school's portal — the primary place where students register for classes, pay bills, and otherwise manage their financial relationship to the university. That is, until a surge in successful phishing attacks resulted in several students having bank accounts and W-2 tax forms siphoned.

Attribution 1 Publication: krebsonsecurity.com / NY AG's office Author:
Article Title: Phishing 101 at the School of Hard Knocks
Article URL: https://krebsonsecurity.com/tag/bowling-green-state-university/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-08	Estill County Chiropractic	KY	3/27/2017	Electronic	Medical/Healthcare	Yes - Published #	5,335

On January 17, 2017, Estill County Chiropractic ("ECC") discovered that an unauthorized user installed malicious software on its computer system that encrypted patient files. The types of information that may have been viewed during this time frame include patient names, email addresses, phone numbers, addresses, dates of birth, Social Security numbers, clinical information, provider notes, diagnosis information, claims, and health plan numbers.

Attribution 1 Publication: databreaches.net / ECC website / hhs.g Author:
Article Title: Estill County Chiropractic notifies 5,335 patients of ransomware attack
Article URL: https://www.databreaches.net/ky-estill-county-chiropractic-notifies-5335-patients-of-ransomware-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-07	Washington University School of Medicine	SC	3/28/2017	Electronic	Educational	Yes - Published #	80,270

On January 24, 2017, the medical school learned that some of its employees responded to a Dec. 2, 2016, "phishing" email, believing it to be a legitimate request. We conducted a detailed review of the employees' email accounts and confirmed that some of the emails contained patient information, which may have included names, birth dates, medical record numbers, diagnosis and treatment information, other clinical information, and in some instances Social Security numbers.

Attribution 1 Publication: School Website / databreaches.net / hhs Author:
Article Title: Washington University School of Medicine
Article URL: https://medicine.wustl.edu/news/announcements/notice-patients-email-phishing-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-06	Araca Merchandise, L.P. / The Araca Group	NY	3/24/2017	Electronic	Business	Yes - Published #	551

We recently discovered that our company was the victim of an email spoofing attack on January 31, 2017, by an individual or individuals pretending to be our Chief Executive Officer. An email request was received from someone who appeared to be Araca's CEO, asking for 2016 Araca employee W-2 information. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / CT AG's office / NY AG' Author:
Article Title: Araca Merchandise, L.P. / The Araca Group
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Araca%20-%20Vermont%20Regulator%20Notice.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-05	Walton School District	FL	3/21/2017	Electronic	Educational	Yes - Unknown #	Unknown

"Well we were victims of basically a very elaborate phishing scheme," said Walton School District Superintendent A. Russell Hughes. "We received an email from an unknown person that was impersonating the superintendent," said Chief Information Officer, Henry Martin.

Attribution 1 Publication: databreaches.net / WJHG.com Author:
Article Title: EXCLUSIVE: Walton School District falls victim to scam
Article URL: http://www.wjhg.com/content/news/EXCLUSIVE-Walton-School-District-falls-victim-to-scam--416776183.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-04	Rudd & Company	ID	3/22/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 5, 2017, Rudd & Company, PLLC ("Rudd & Company") dtscovered it was the target of a cyberattack which effected its computer information systems and resulted in unauthorized access to data files whlch may have contained your personal information mcluding name, address, birth date, Social Security number, and financial account information.

Attribution 1 Publication: MT AG's office Author:
Article Title: Rudd & Company
Article URL: https://dojmt.gov/wp-content/uploads/Rudd-Company.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-03	Mollie Stone's Markets	CA	3/23/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 17, 2017, we learned that one of our employees received a phishing email designed to appear as if it came from one of our Senior Executives. As a result of this phishing incident, we learned that an unauthorized individual may have obtained IRS Form W-2s for the 2016 employment year for some of our employees.

Attribution 1 Publication: CA AG's office Author:
Article Title: Mollie Stone's Markets
Article URL: https://oag.ca.gov/system/files/redacted_MSM_Letter%20to%20Adults_Redacted_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-02	Easy Breathe, Inc.	CA	3/27/2017	Electronic	Business	Yes - Published #	78,759

On February 10, 2017, we learned that an unknown individual may have accessed your credit or debit card information used to make purchases at our online store. (Exposure number per NY AG's)

Attribution 1 Publication: CA AG's office / OR AG's office / NH AG Author:
Article Title: Easy Breathe, Inc.
Article URL: https://oag.ca.gov/system/files/Easy%20Breathe%20notice%20only0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170328-01	Daytona State College #2	FL	3/27/2017	Electronic	Educational	Yes - Unknown #	Unknown

Daytona State College students who applied for financial aid might find themselves in a financial mess. The school said a data breach involving financial aid forms means thieves could have personal information needed to steal students' identities. It marks the second security breach involving the school.

Attribution 1 Publication: WFTV.com / NH AG's office Author:
Article Title: Data breach may put Daytona State College students' personal info at risk
Article URL: http://www.wftv.com/news/local/data-breach-may-put-daytona-state-college-students-personal-info-at-risk/506505427

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170327-03	**Lane Community College Health Clinic**	OR	3/23/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,911**

A technician at Lane Community College health clinic recently discovered a computer virus, which may have exposed the PHI of some patients, according to an online statement. The Oregon college health clinic stated the virus may have been sending the names, addresses, phone numbers, diagnoses, and Social Security numbers to an unknown third party for over a year.

Attribution 1 Publication: healthitsecurity.com / OR AG's office Author:
Article Title: Computer Virus Potentially Exposes PHI of 2.5K at OR Clinic
Article URL: http://healthitsecurity.com/news/computer-virus-potentially-exposes-phi-of-2.5k-at-or-clinic

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170327-02	**Commonwealth Health Corporation / Med Center**	AL	3/23/2017	Electronic	Medical/Healthcare	Yes - Published #	**697,800**

The FBI continues its look into a breach of personal information from about 160,000 patients serviced at some Med Center Health affiliates between 2011 and 2014. A former employee is accused of taking the data that included billing information such as name, address, Social Security, insurance information, procedure codes and others. (Commonwealth Health) (Exposure number per HHS)

Attribution 1 Publication: bgdailynews.com / MT AG's office / hipa Author:
Article Title: 160K affected by Med Center data breach
Article URL: http://www.bgdailynews.com/news/k-affected-by-med-center-data-breach/article_d593a66b-c453-5ab7-8e25-75b599de6

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170327-01	**Krystle Property Management, Inc.**	CA	3/24/2017	Electronic	Business	Yes - Unknown #	**Unknown**

“On Dec. 28, an unknown individual gained access to our server in what is known as a ransomware attack,” the letter says. “After combing through our 80 gigabytes of backup recovery files, there were just a few documents that were of concern. The attack involved a shared hard drive at Krystle’s Tennessee Street office, containing more than 80 gigabytes of data, comprised mainly of JPEG files of properties for inspection and advertising purposes, encrypted files for previous property management software and various letters and excel documents,” according to the letter.

Attribution 1 Publication: timesheraldonline.com Author:
Article Title: Data breach at local property management firm leaves unknown number at risk
Article URL: http://www.timesheraldonline.com/general-news/20170324/data-breach-at-local-property-management-firm-leaves-unk

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-26	**VWSE Productions, LLC**	NY	3/15/2017	Electronic	Business	Yes - Published #	**848**

VWSE Productions, LLC is writing to inform you that on January 23, 2017 we were notified that a company laptop and removable disc drive were stolen from one of our employees. We have identified that the laptop computer and removable disc drive may have contained files with some of our employees' and contractors' personal information, including first and last name, social security number and in some cases, address. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: VWSE Productions, LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/vwse-20170315.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-25	**Comfort Technology / Therafit Shoes**	FL	3/6/2017	Electronic	Business	Yes - Published #	**445**

On February 21, 2017, Therafit discovered that an unknown individual may have accessed the credit or debit card information customers typed into its website for the purpose of making a purchase from itsonline store, www.therafitshoe.com. Therafit determined that the unknown individual may have accessed customer payment card information, including name, address, telephone number, and credit or debit card information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / NY AG Author:
Article Title: Comfort Technology / Therafit Shoes
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/therafit-shoes-20170316.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-24	Rand McNally / RM Acquisition	IL	3/17/2017	Electronic	Business	Yes - Published #	21,237

On February 28, 2017 our client discovered an external systems breach due to malware that was installed in its ecommerce website software. The personal information subject tounauthorized access during the breach included consumer names, user names and/or email addresses, and credit or debit card numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / CA AG's office / MT AG' Author:
Article Title: Rand McNally
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/rand-mcnally-20170316.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-23	RealTruck, Inc.	ND	3/17/2017	Electronic	Business	Yes - Unknown #	Unknown

In late January of this year, RealTruck detected suspicious activity on one of its web servers. After detecting the activity, RealTruck launched an immediate review to determine the scope of the incident and what data
may have been impacted. RealTruck has since determined that an intrusion into one of its servers had occurred on or around January 22, 2017.

Attribution 1 Publication: NH AG's office Author:
Article Title: RealTruck, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/realtruck-20170317.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-22	Russell Investments	WA	3/7/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 22, 2017, Russell Investments discovered that it experienced a data breach when a Russell Investments associate sent files containing personally identifiable information ("PII") to a personal Gmail account and downloaded those files to a personal computing device.

Attribution 1 Publication: NH AG's office Author:
Article Title: Russell Investments
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/russell-investments-20170307.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-21	Principal Finacial Group	IA	3/13/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

The incident was identified on March 2, 2017 when we were notified by our eBenefits platform vendor that files were sent in error to Chard Snyder, a third party COBRA vendor. The information included the name, address, home phone number, Social Security number, and COBRA eligibility information.

Attribution 1 Publication: NH AG's office Author:
Article Title: Principal Finacial Group
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/principal-financial-20170313.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-20	netPolarity, Inc.	CA	3/17/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 2, 2017, a netPolarity employee received a "phishing" email that appeared to come from netPolarity's CEO and that instructed the employee to provide W-2 forms in response. The employee mistakenly responded to this email by sending W-2 forms, including yours, as an attachment.

Attribution 1 Publication: NH AG's office Author:
Article Title: netPolarity, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/netpolarity-20170317.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-19	Maxim Crane Works / Amquip	PA	3/15/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 22, 2017, the Company confirmed that an Amquip administrator had received a fraudulent email disguised as a legitimate one. The employee responded to the email request believing it to be a legitimate, and the personal information, including name, address, income information, and Social Security numbers, of certain Amquip employees was released.

Attribution 1 Publication: NH AG's office Author:
Article Title: Maxim Crane Works
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/maxim-crane-20170315.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-18	inMoment, Inc.	UT	3/14/2017	Electronic	Business	Yes - Published #	246

Based upon our investigation, it appears that on January 27, 2017, an unauthorized individual, impersonating an InMoment executive, contacted an InMoment employee requesting 2016 W-2 information for certain current and former InMoment employees. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: inMoment, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/inmoment-20170314.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-17	inTest Corporation / Temptronic Corporation	NJ	3/13/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 27, 2017, inTEST first learned that the W2 information of Temptronic employees was compromised through an email phishing attack on January 23, 2017.

Attribution 1 Publication: NH AG's office Author:
Article Title: inTest Corporation
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/intest-20170313.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-16	HealthTexas Provider Network	TX	3/10/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On January 11, 2017, our client, HealthTexas Provider Network ("HTPN"), which includes Denton Heart Group (the "Clinic"), learned that an external computer hard drive was stolen from the Clinic on or about December 29, 2016. It may have included certain demographic information (such as name, date of birth, address and phone number), medical record number, clinic account number, insurance provider's name, insurance group and/or policy numbers, physician's name and clinical information related to medical care received at the Clinic between 2009 and 2016.

Attribution 1 Publication: NH AG's office Author:
Article Title: HealthTexas Provider Network
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/healthtexas-20170310.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-15	Bacon & Company CPAs, LLC	RI	2/16/2017	Electronic	Business	Yes - Published #	1,157

Based on our investigation to date, we believe unauthorized person(s) hacked into our computer information system and used data on the system to fraudulently file income tax returns.On February 20, 2017, Bacon & Company CP As, LLC ("Bacon & Company") discovered a data security incident which resulted in unauthorized access to data files which may have contained your personal information including name, address, birth date, Social Security number, and fmancial account information.

Attribution 1 Publication: MA OCABR / ME AG's office / NY AG's Author:
Article Title: Bacon & Company CPAs, LLC
Article URL: NY AG's office FOIA request

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-14	Berg LLC	MA	3/21/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 16, 2017, Berg LLC ("Berg"), a Boston-based biopharma company, became aware that an unknown individual fraudulently obtained access to its employees ' W-2 information.

Attribution 1 Publication: NH AG's office / ME AG's office Author:
Article Title: http://www.doj.nh.gov/consumer/security-breaches/documents/berg-20170321.pdf
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/berg-20170321.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-13	Federal Process Corporation	OH	2/27/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 23, 2017, the company learned that an unauthorized third party obtained a copy of your IRS W-2 Form through a fraudulent email scheme. As a result, some of your personal information has been compromised.

Attribution 1 Publication: OR AG's office Author:
Article Title: Federal Process Corporation
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1756333624

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-12	Allina Health System	MN	2/23/2017	Paper Data	Medical/Healthcare	Yes - Published #	776

Allina Health System MN Healthcare Provider 776 02/23/2017 Improper Disposal Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Allina 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
ITRC20170324-11	FIRST For the Inspiration and Recognition of Science and	NH	3/24/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 6, 2017, we received a report of suspicious activity for our two externally hosted websites – the FIRST Forum (forums.usfirst.org) and FIRST Tech Challenge Forum (ftcforum.usfirst.org). While our investigation into this incident is ongoing, participant information may have included your username (defined by you, which may or may not include your first or last name), email address, date of birth, and encrypted password.

Attribution 1 Publication: CA AG's office Author:
Article Title: FIRST For the Inspiration and Recognition of Science and Technology
Article URL: https://oag.ca.gov/system/files/FIRST%20-%20CA%20Notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-10	Affiliated Sante Group	MD	1/31/2017	Electronic	Medical/Healthcare	Yes - Published #	550

The Affiliated Sante Group MD Healthcare Provider 550 01/31/2017 Unauthorized Access/Disclosure Electronic Medical Record

Attribution 1 Publication: hhs.gov Author:
Article Title: Affiliated Sante 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
ITRC20170324-09	Primary Care Specialists	TN	3/9/2017	Electronic	Medical/Healthcare	Yes - Published #	65,000

Primary Care Specialists, Inc. TN Healthcare Provider 65000 03/09/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Primary Care Specialists
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=97705530101B7DBF9B46036D8DB73F88

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-07	American Home Patient	TN	3/6/2017	Electronic	Medical/Healthcare	Yes - Published #	13,861

On January 7, 2017, we discovered that our American HomePatient office in Newark, Delaware had been burglarized. Several computer hard drives containing personal information were stolen from the office during the burglary. The stolen computers involved in this incident may have contained first and last names, addresses, American HomePatient account numbers, Social Security Numbers, diagnosis codes, date of birth, financial information, and treatment information.

Attribution 1 Publication: hhs.gov / MD AG's office Author:
Article Title: American Home Patient
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280518%20(1).pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-06	Metropolitan Urology Group	WI	3/10/2017	Electronic	Medical/Healthcare	Yes - Published #	17,634

Wauwatosa, WI-based Metropolitan Urology Group has recently discovered a ransomware attack that affected two computer servers potentially resulted in the attackers gaining access to the protected health information of 17,634 patients.

Attribution 1 Publication: hhs.gov / hipaajournal.com / WI AG's off Author:
Article Title: Almost 18,000 Metropolitan Urology Patients Impacted by Ransomware Attack
Article URL: http://www.hipaajournal.com/almost-18000-metropolitan-urology-patients-impacted-ransomware-attack-8733/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-05	Houston Methodist Cancer Center	TX	3/17/2017	Electronic	Medical/Healthcare	Yes - Published #	1,416

"On March 9, 2017, one of our employees unintentionally disclosed your email address to 1,416 other patients, and associated it with the Houston Methodist Cancer Center while requesting follow-up information," stated the letter, a copy of which was posted by the Houston Chronicle.

Attribution 1 Publication: healthitsecurity.com Author:
Article Title: Houston Methodist Cancer Center sends email revealing patient data
Article URL: http://healthitsecurity.com/news/computer-virus-potentially-exposes-phi-of-2.5k-at-or-clinic

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-04	Rocky Mountain Health Maintenance	CO	3/17/2017	Paper Data	Medical/Healthcare	Yes - Published #	1,320

Rocky Mountain Health Maintenance Organization, Inc. CO Health Plan 1320 03/17/2017 Unauthorized Access/Disclosure Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-03	Highland Rivers Community Service Board	GA	3/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	967

Highland Rivers Community Service Board GA Healthcare Provider 967 03/20/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Highland Rivers Community Service Board
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-02	Urology Austin, PLLC	TX	1/22/2017	Electronic	Medical/Healthcare	Yes - Published #	279,663

On January 22, 2017, Urology Austin was the victim of a ransomware attack that encrypted the data stored on our servers. Our investigation indicates that your personal information may have been impacted by the ransomware, including your name, address, date of birth, Social Security number, and medical information.

Attribution 1 Publication: CA AG's office / VT AG's office / MT AG' Author:
Article Title: Urology Austin
Article URL: https://oag.ca.gov/system/files/Urology%20Austin%20-notice%20only_0.pdf?

Attribution 2 Publication: healthcareinfosecurity.com / hipaajourna Author:
Article Title: Texas Specialty Practice Suffers Ransomware Attack
Article URL: http://www.healthcareinfosecurity.com/texas-specialty-practice-suffers-ransomware-attack-a-9797?rf=2017-03-28_ENE

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170324-01	Schurman Retail Group	CA	3/21/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 8, 2017, we discovered that our company was the victim of an email spoofing attack on January 18, 2017, by an individual pretending to be our Chief Financial Officer. A request was made from what appeared to be a legitimate Schurman Retail Group ("SRG") email address for all 2016 SRG employee Form W-2 information.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Schurman Retail Group
Article URL: https://oag.ca.gov/system/files/SRG%20--%20Notice%20only%20-%20Regulator%20Notice%20CA%20%28002%29_0.pd

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-14	America's Joblink Alliance	KS	3/21/2017	Electronic	Government/Military	Yes - Published #	5,500,000

The Joblink system, which is also used by nine other states, is a standalone system and is not linked to any other State of Vermont systems. Initial details indicate this was a systematic breach designed to extract data from Joblink, and it is unknown whether the software was deliberately inserted or the result of an unintentional introduction by a jobseeker with an infected computer.

Attribution 1 Publication: esecurityplanet.com Author:
Article Title: Massive Data Breach Exposes 4.8 Million Job Seekers' Personal Info
Article URL: http://www.esecurityplanet.com/network-security/massive-joblink-breach-exposes-4.8-million-job-seekers-personal-da

Attribution 2 Publication: AJLA press release Author:
Article Title: America's Joblink Alliance
Article URL: http://www.ajla.net/pressrelease.html

Attribution 3 Publication: kfdi.com Author:
Article Title: Data breach at America's JobLink affects Kansans
Article URL: http://www.kfdi.com/news/data-breach-at-americas-joblink-affects-kansans

Attribution 4 Publication: databreaches.net / vermontbiz.com Author:
Article Title: America's Joblink Alliance
Article URL: http://www.vermontbiz.com/news/march/vermont-department-labor-details-data-security-breach-third-party-vendor

Attribution 5 Publication: chicagotribune.com Author: 7/21/2017
Article Title: Hackers of Kansas system had access to millions of Social Security numbers in 10 states
Article URL: http://www.chicagotribune.com/news/nationworld/midwest/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-13	Coupa	CA	3/20/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 6, according to the letter sent to the workers and obtained by SiliconBeat, the firm's human resources department was targeted in a successful phishing fraud seeking employee's IRS W-2 payroll forms. (Exposure number per NY AG's office)

Attribution 1 Publication: databreaches.net / siliconbeat.com / NY Author:
Article Title: Fraudster impersonates CEO of $1.2 billion San Mateo tech firm, steals employees' SSNs and other IRS data
Article URL: http://www.siliconbeat.com/2017/03/20/irs-data-for-employees-of-1-2-billion-san-mateo-software-firm-stolen-in-fake-ce

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-12	Palm Bay International	NY	2/28/2017	Electronic	Business	Yes - Published #	362

On January 17, 2017, one of our employees emailed the IRS Form W-2 information of one (I) current or former New Hampshire employee in response to what they later learned was a fraudulent email purporting to be from our CEO requesting the information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / NY AG Author:
Article Title: Palm Bay International
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/palm-bay-20170228.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-11	J.N. Phillips Company, Inc.	MA	3/17/2017	Electronic	Business	Yes - Published #	573

On February 16, 2017 an unknown, unauthorized person from outside of J.N. Phillips impersonated a member of J.N. Phillips management and, using what appeared to be that person's legitimate J.N. Phillips email address, convinced one of our employees to provide certain personal information about all personnel of The J.N. Phillips Company, Inc., Windshield Centers LLC and Strategic Claim Services, Inc. employed during the 2016 tax year. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / ME AG's office / CT AG' Author:
Article Title: J.N. Phillips Company, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/jn-phillips-20170317.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-10	People for People	WA	3/16/2017	Electronic	Business	Yes - Unknown #	Unknown

The morning of Thursday, October 20, 2016, we discovered that an unauthorized individual briefly gained access to the email account for one of our employees. Upon discovery, we immediately secured the email account. The information that may have been accessed includes names, addresses, dates of birth, Driver's License numbers, and Social Security numbers.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-09	Office of Shelia A. Wilson-Alexander	KY	3/20/2017	Electronic	Business	Yes - Unknown #	Unknown

We recently fell victim to a compromise of our remote access server on March 3, 2017, which resulted in the disclosure of your tax documents. This information includes name, address and social security number.

Attribution 1 Publication: VT AG's office Author:
Article Title: Office of Shelia A. Wilson-Alexander
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Shelia%20A.%20Wilson-Alexander%20CPA%20SBN%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-08	LYFE Kitchen Companies, LLC	TN	1/6/2017	Electronic	Business	Yes - Unknown #	Unknown

LYFE Kitchen was notified by its third-party point of sale ("POS") vendor that the vendor's computer network potentially had been compromised by a malware data breach.

Attribution 1 Publication: CA AG's office Author:
Article Title: LYFE Kitchen Companies, LLC
Article URL: https://oag.ca.gov/system/files/LYFE%20Kitchen%20Notice%20of%20Data%20Breach_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-07	**Rent the Runway**	NY	2/23/2017	Electronic	Business	Yes - Unknown #	**Unknown**

It was discovered that your Rent the Runway account was accessed by an unknown party between December 25, 2016 and February 23, 2017.The information that may have been accessed includes: email address, first name, last name, birthday and mailing address.

Attribution 1 Publication: CA AG's office Author:
Article Title: Rent the Runway
Article URL: https://oag.ca.gov/system/files/ca_notice_sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-06	**PoliceOne forums**	CA	2/7/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On Friday, February 3, 2017, we were notified that the content of our PoliceOne Forum was the subject of unauthorized access and acquisition. The information accessed was limited, and included email addresses, user names and hashed and salted passwords (a protected version of the password you use). It did not include forums posts or other content.

Attribution 1 Publication: CA AG's office Author:
Article Title: PoliceOne forums
Article URL: https://oag.ca.gov/system/files/Praetorian%20Digital%20notice%20only%20CA_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-05	**Bulletproof 360, Inc.**	WA	3/21/2017	Electronic	Business	Yes - Published #	**28,033**

After noticing unusual activity relating to customer online transactions, we began an immediate investigation of our website and took prompt action to address and stop the unauthorized activity. On February 23, 2017, our investigation determined that an unknown third party had compromised our e-commerce system, potentially affecting customer payment card information. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NH AG' Author:
Article Title: Bulletproof 360, Inc.
Article URL: https://oag.ca.gov/system/files/BPF%20CA%20Sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-04	**Select Restaurants, Inc.**	OH	3/16/2017	Electronic	Business	Yes - Unknown #	**Unknown**

For the second time in the past nine months, Google has inadvertently but nonetheless correctly helped to identify the source of a large credit card breach — by assigning a “This site may be hacked” warning beneath the search results for the Web site of a victimized merchant.

Attribution 1 Publication: CA AG's office Author:
Article Title: Select Restaurants, Inc.
Article URL: https://oag.ca.gov/system/files/Select%20-notice%20only_0_1.pdf?

Attribution 2 Publication: krebsonsecurity.com / CA AG's office / Author:
Article Title: Google Points to Another POS Vendor Breach
Article URL: https://krebsonsecurity.com/2017/03/google-points-to-another-pos-vendor-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-03	**University of North Carolina Health Care**	NC	3/20/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,300**

UNC Health Care said Monday it has begun notifying patients of a potential breach where personal data provided by prenatal patients at two obstetric clinics were mistakenly transmitted to local county health departments. The forms may have included Social Security numbers and details about physical and mental health history, including HIV status and any sexually transmitted diseases, officials said.

Attribution 1 Publication: wral.com / hipaajournal.com Author:
Article Title: Data breach may involve hundreds of UNC Health prenatal patients
Article URL: http://www.wral.com/data-breach-may-involve-hundreds-of-unc-health-prenatal-patients/16596295/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-02	Saks Fifth Avenue	NY	3/19/2017	Electronic	Business	Yes - Unknown #	Unknown

Saks Fifth Avenue is the latest retailer to report that customers' personal information has been inadvertently exposed online. In this case, it was e-mail addresses and phone numbers of Saks shoppers that were visible on its retail website.

Attribution 1 Publication: usatoday.com Author:
Article Title: Personal data of Saks customers exposed
Article URL: http://www.usatoday.com/story/money/markets/2017/03/19/saks-customers-data-exposed/99387274/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170321-01	Powhatan County Public Schools	VA	3/20/2017	Electronic	Educational	Yes - Published #	900

Powhatan County Public Schools is scrambling to protect its employees after it was learned that a data breach from a possible phishing scam occurred today that led to more than 900 W-2s being compromised. The breach happened when a payroll employee responded to an email phishing scam requesting employees' W-2 forms for 2016, Dr. Eric Jones, superintendent, said in a phone interview.

Attribution 1 Publication: richmond.com Author:
Article Title: Financial records of 905 Powhatan schools employees compromised
Article URL: http://www.richmond.com/news/local/central-virginia/powhatan/powhatan-today/financial-records-of-powhatan-school

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170320-07	Biomedical Systems Corp.	MO	3/13/2017	Electronic	Business	Yes - Unknown #	Unknown

A criminal posing as a member of Biomedical Systems' management team obtained copies of Biomedical Systems' employees' Form W-2 for 2016.

Attribution 1 Publication: NH AG's office Author:
Article Title: Biomedical Systems Corp.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/biomedical-20170313.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170320-06	SolutionsIQ, Inc.	WA	3/10/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 28, 2017, an email with an attachment contammg personal information of individuals employed in 2016 by our client, SolutionsIQ, Inc. ("SolutionsIQ"), was inadvertently shared with an unauthorized recipient because of an email phishing scam. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: SolutionsIQ, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/solutionsiq-20170310.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170320-05	Defense Point Security	VA	3/17/2017	Electronic	Business	Yes - Unknown #	Unknown

On Thursday, March 16, the CEO of Defense Point Security, LLC — a Virginia company that bills itself as "the choice provider of cyber security services to the federal government" — told all employees that their W-2 tax data was handed directly to fraudsters after someone inside the company got caught in a phisher's net.

Attribution 1 Publication: krebsonsecurity.com / MD AG's office / Author:
Article Title: Govt. Cybersecurity Contractor Hit in W-2 Phishing Scam
Article URL: https://krebsonsecurity.com/2017/03/govt-cybersecurity-contractor-hit-in-w-2-phishing-scam/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170320-04	**Campbell Taylor & Company (multiple clients)**	CA	3/21/2017	Electronic	Business	Yes - Published #	**19,472**

After noticing some unusual activity on our network including a possible ransomware attempt, on February 13, 2017, we hired a specialized forensic IT firm to investigate. As an employee participant of a retirement or other benefit plan, the information on our system may have included your: first and last name, date of birth, Social Security number, and salary information. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG'soffice Author:
Article Title: Performant Financial Corporation
Article URL: https://oag.ca.gov/system/files/Sample%20Performant%20Notice%20to%20Individuals%20-%20CT%20Data%20Breach

Attribution 2 Publication: CA AG's office / MT AG's office / NY AG' Author:
Article Title: Campbell Taylor & Company (multiple clients)
Article URL: https://oag.ca.gov/system/files/Campbell%20EBP%20Notification%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170320-03	**Hampton Jitney Inc.**	NY	2/20/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On February 22, 2017, we discovered that an unauthorized user recently accessed customer accounts at Hampton Jitney. Information including customer names, addresses, phone numbers, email addresses and unencrypted passwords was accessible for two days.

Attribution 1 Publication: CA AG's office Author:
Article Title: Hampton Jitney Inc.
Article URL: https://oag.ca.gov/system/files/CA_email_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170320-02	**American Tire Distributors Holdings, Inc.**	NC	3/3/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We believe that on March 3, 2017 a file containing your 2016 W-2 information was apparently fraudulently obtained by a third party. We learned of this on March 6, 2017 and an investigation immediately
commenced. We believe the incident has been contained and did not involve an intrusion into the company's networks.

Attribution 1 Publication: CA AG's office / NH AG's office / ME AG Author:
Article Title: American Tire Distributors Holdings, Inc.
Article URL: https://oag.ca.gov/system/files/American%20Tire%20Security%20Breach%20Notification%20-%20NOTICE%20ONLYCA

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170320-01	**Zest Dental Solutions**	CA	3/16/2017	Electronic	Medical/Healthcare	Yes - Published #	**4,806**

On February 16, 2017, we learned that an unauthorized entity had compromised our e-commerce system, potentially affecting customer payment card information. The information compromised by the attack may have included your name, billing address, phone number, payment card number, expiration date, and CW number from payment cards used for online transactions on Zest Dental's website between December 31 , 2013 and September 21 , 2014, and between November 2, 2016 and February 4, 2017. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / NY AG' Author:
Article Title: Zest Dental Solutions Alerts Customers to Payment Card Information Breach
Article URL: http://www.hipaajournal.com/zest-dental-solutions-alerts-customers-payment-card-information-breach-8730/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-17	**Arkansas City USD 470**	KS	3/15/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

Ballard says an innocent-looking email recently came into several employees in his district. Someone who looked like a legitimate employee was requesting information. But, it turns out, the email was from scammers, who were phishing for social security numbers and personal information.

Attribution 1 Publication: databreaches.net / ksn.com Author:
Article Title: Phishing scam hits Arkansas City schools, FBI and IRS investigating
Article URL: http://ksn.com/2017/03/14/phishing-scam-hits-ark-city-schools-fbi-and-irs-investigating/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-16	Ben Bolt Independent School District	TX	3/15/2017	Electronic	Educational	Yes - Unknown #	Unknown

According to the Jim Wells County Sheriff's Department, school administrators with Ben Bolt I.S.D. emailed W-2 forms and employee information to a person posing as the superintendent.

Attribution 1 Publication: databreaches.net / kristv.com Author:
Article Title: School administrators fall victim to possible scam
Article URL: http://www.kristv.com/story/34900335/school-administrators-fall-victim-to-possible-scam

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-15	Toscano Clements Taylor	NY	3/5/2017	Electronic	Business	Yes - Unknown #	Unknown

On Friday, March 3, 2017, our accounts payable employee received an email that appeared to be from me. The email looked to be legitimate. It asked t he employee to send me the 2016 W-2 information. At 11.52 a.m. the employee responded to the email, thinking the response was being sent to me. The response included W-2 information on all current and former employees that worked for TCT in 2016.

Attribution 1 Publication: NH AG's office / MD AG's office / ME A Author:
Article Title: Toscano Clements Taylor
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/toscano-clements-taylor-20170305.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-14	Dairy Management, Inc.	IL	3/7/2017	Electronic	Business	Yes - Unknown #	Unknown

On Thursday, February 9, 2017 Dairy Management Inc. was the target of a data breach involving employees' W-2 information. Compromised information included employees' names, addresses, Social Security numbers and current earnings.The breach was discovered when two employees attempted to electronically file their 2016 tax returns, and they were rejected by the IRS.

Attribution 1 Publication: WI AG's office Author:
Article Title: Dairy Management, Inc.
Article URL: https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-13	Berkley Mid-Atlantic Group	VA	3/15/2017	Electronic	Business	Yes - Unknown #	Unknown

We were recently the victims of a social engineering scam which resulted in the exposure of your 2016 W-2 information, including your name, address, social security number and salary information.

Attribution 1 Publication: Databreaches.net / BMAG notification Author:
Article Title: More reports of false tax returns in wake of W-2 phishing scams
Article URL: https://www.databreaches.net/wp-content/uploads/BerkleyMAG_Notification.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-12	St. Charles Health System	OR	3/16/2017	Electronic	Medical/Healthcare	Yes - Published #	2,459

On January 16, 2017, St. Charles learned that one of its caregivers accessed a patient's record without authorization. While the investigation is ongoing, St. Charles believes that the caregiver accessed your information, which may have included your name, address, date of birth, health insurance information and medical information such as diagnostic information, treating physician name, medical history, medications and treatment information.

Attribution 1 Publication: OR AG's office / hhs.gov / hipaajournal.c Author:
Article Title: St. Charles Health System
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1462011573

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-11	**Local 693 Plumbers & Pipefitters Health & Welfare**	VT	3/9/2017	Electronic	Business	Yes - Published #	**1,291**

The back-up hard drive was first identified as missing on January 23, 2017, following discovery that our offices had been broken into. Among the data maintained on the back-up hard drive were individualized records of 1,291 current and former plan participants, beneficiaries and union members. Accordingly, we believe your personal information was contained on the stolen device. Among the information contained on the back-up hard drive was personal information (including personal health information) including full names, addresses, telephone numbers, and social security numbers.

Attribution 1 Publication: VT AG's office / hhs.gov / hipaajournal.c Author:
Article Title: Plumbers & Pipefitters Local 693
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/UA%20Local%20693%20Plumbers%20and%20Pipefitte

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-10	**QualiChem**	VA	3/9/2017	Electronic	Business	Yes - Published #	**84**

In particular, in on February 13, 2017 an employee fell victim to a fraudulent email phishing scheme requesting W-2 wage information. The QualiChem employee sent the W-2 information of QualiChem's employees (approximately 84 individuals) in response to the fraudulent email. Only one of those employees resides in New Hampshire.

Attribution 1 Publication: NH AG's office / WI AG's office Author:
Article Title: QualiChem
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/qualichem-20170309.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-09	**Tyler Technologies**	TX	3/13/2017	Electronic	Business	Yes - Published #	**7,788**

On March 3, 2017, an employee inadvertently sent an email attachment containing personal information to a limited number of recipients who were not authorized to receive this information. From our review, it appears the file may have contained your name, address, Social Security number, and income information. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / NY AG' Author:
Article Title: Tyler Technologies
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Tyler%20Technologies%20Inc%20SBN%20to%20Cons

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-08	**Northwest Christian Schools, Inc.**	WA	3/16/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

On February 13, 2017, NWCS learned of a data security incident that may have affected your personal information. Immediately upon learning of the incident, NWCS disabled access to the servers which stored the information and engaged its information technology provider to complete a rebuild of its computer systems. The following personal information may have been accessed without authorization – employee names, addresses, dates of birth, Social Security numbers, and banking information.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-07	**Colorado Nonprofit Development Center**	CO	3/3/2017	Electronic	Business	Yes - Unknown #	**Unknown**

You may have heard in the news that there has been an email scam to get employee W-2s. Unfortunately, this afternoon CNDC was caught in that scam, possibly impacting employees who worked for CNDC/Projects in 2016.

Attribution 1 Publication: MT AG's office Author:
Article Title: Colorado Nonprofit Development Center
Article URL: https://dojmt.gov/wp-content/uploads/Colorado-Nonprofit-Development-Center.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-06	Ameriprise Financial (3/17)	MN	3/17/2017	Electronic	Banking/Credit/Financial	Yes - Published #	687

In December of 2016 a staff member uploaded a copy of a client list to an application In Google, to facilitate sharing the list among the office. Unfortunately, that list included personal information, in particular, it contained your name and Social Security Number. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office / NY AG' Author:
Article Title: Ameriprise Financial (3/17)
Article URL: https://dojmt.gov/wp-content/uploads/Ameriprise-Financial-Services-Inc.-3.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-05	Vertex Wireless, Inc.	AZ	3/17/2017	Electronic	Business	Yes - Published #	1,838

On February 21, 2017, we determined that our server may have been accessed by an unknown, unauthorized individual. We immediately took action to secure our system and commenced an investigation to determine what information may have been accessed. We determined that the unknown individual may have accessed your name, address and credit card information. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / VT AG's office / NH AG' Author:
Article Title: Vertex Wireless, Inc.
Article URL: https://dojmt.gov/wp-content/uploads/Vertex-Wireless.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-04	ADF International	MT	3/13/2017	Electronic	Business	Yes - Published #	303

After several ADF International employees reported receiving a Montana Department of Revenue notifications of fraudulent tax returns filed in Montana, we discovered that ADF international, Inc. employee's W-2's for 2016 have been compromised. (Additional details: http://www.doj.nh.gov/consumer/security-breaches/documents/adf-20170412.pdf) (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office / NY AG' Author:
Article Title: ADF International
Article URL: https://dojmt.gov/wp-content/uploads/ADF-International.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-03	City of San Marcos	TX	3/16/2017	Electronic	Government/Military	Yes - Published #	803

Every person employed by the city of San Marcos in 2016 is at risk of identity theft after the city says an employee was targeted in a "spear phishing" email. The city tells KXAN News 803 employees' information was compromised. In an email sent to all city employees, the acting city manager, Steve Parker, says his department learned about the situation on Tuesday. Parker says the city employee responded to a targeted "spear phishing" email on Feb. 22.

Attribution 1 Publication: kxan.com Author:
Article Title: San Marcos city employees at risk of identify theft due to email scam
Article URL: http://kxan.com/2017/03/16/hundreds-of-w2s-stolen-from-city-of-san-marcos-in-email-scam/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-02	Wishbone App	CA	3/16/2017	Electronic	Business	Yes - Unknown #	Unknown

Wishbone, a mobile app that is especially popular with teenage girls, suffered a data breach in August 2016 that compromised 9.4 million records, 2.2 million of which were registered with unique email addresses.

Attribution 1 Publication: scmagazine.com / WI AG's office Author:
Article Title: Wishy-washy security? Wishbone mobile app breached
Article URL: https://www.scmagazine.com/wishy-washy-security-wishbone-mobile-app-breached/article/644723/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170317-01	Classic Tax	IA	3/16/2017	Electronic	Business	Yes - Published #	240

Classic Tax in Marion learned of the breach around February and now clients are finding out if they were a part of it as they file their taxes. The breach is affecting 20 percent of the company's 1,200 clients.

Attribution 1 Publication: kcrg.com Author:
Article Title: Eastern Iowans experience tax fraud after data breach
Article URL: http://www.kcrg.com/content/news/Eastern-Iowans-experience-tax-fraud-after-data-breach--416393623.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170316-03	Geokinetics	TX	3/13/2017	Electronic	Business	Yes - Published #	709

On March 6, 2017, we learned that Geokinetics 2016 W-2s, including yours, were sent out on January 25, 2017 outside the organization. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / MD AG's office / NY AG Author:
Article Title: Geokinetics
Article URL: https://dojmt.gov/wp-content/uploads/Geokinetics.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170316-02	NSC Technologies	VA	3/6/2017	Electronic	Business	Yes - Unknown #	Unknown

On March 2, 2017 an on-line hacker posing as NSC's CEO emailed the company's payroll department and directed that copies of employee W-2 forms be sent to him.

Attribution 1 Publication: CA AG's office Author:
Article Title: NSC Technologies
Article URL: https://oag.ca.gov/system/files/NSC%20Data%20Breach_CA%20Letter_030717_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170316-01	Dun & Bradstreet / NetProspex	NJ	3/15/2017	Electronic	Business	Yes - Unknown #	Unknown

A Dun & Bradstreet 52GB database containing about 33.6 million records with very specific details about each of the people involved from job title to email address has been exposed.

Attribution 1 Publication: scmagazine.com Author:
Article Title: Dun & Bradstreet database breached, 33.6M files vulnerable
Article URL: https://www.scmagazine.com/dun-bradstreet-database-breached-336m-files-vulnerable/article/644419/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170314-04	Ark City School District	KS	3/13/2017	Electronic	Educational	Yes - Unknown #	Unknown

The Ark City school district and its employees were recently the victims of an online phishing scheme in which certain employees' tax account information was compromised.

Attribution 1 Publication: databreaches.net / newscow.net Author:
Article Title: AC school district victim of Internet phishing
Article URL: http://www.newscow.net/story.php?StoryID=12824

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170314-03	BBB Industries	AL	3/10/2017	Electronic	Business	Yes - Published #	444

Yesterday (March 9, 2017), as the result of a phishing scheme, your 2016 W-2 statement was wrongfully obtained by unknown persons outside of the BBB Industries organization. Since recognizing that the W-2 statement was wrongfully released, we have been notifying the appropriate governmental entities, including the Federal Bureau of Investigation, Internal Revenue Service, the state departments of revenue, and the local authorities. (Exposure number per NY AG's office)

Attribution 1 Publication: OR AG's office / NY AG's office Author:
Article Title: BBB Industries
Article URL: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/2029465048

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170314-02	U.S. Air Force	CO	3/14/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

MacKeeper researchers recently discovered that sensitive U.S. Air Force Data was being made available online by a misconfigured backup device. The data appears to have belonged to an Air Force lieutenant who didn't realize it wasn't secured. The exposed data included the names, ranks and Social Security numbers of several hundred service members, as well as Defense Information Systems instructions for recovering encryption keys, and the login URL, user ID and password for the lieutenant's Joint Personnel Adjudication System (JPAS) account.

Attribution 1 Publication: esecurityplanet.com Author:
Article Title: Misconfigured Backup Drive Exposes Sensitive U.S. Air Force Data
Article URL: http://www.esecurityplanet.com/network-security/misconfigured-backup-drive-exposes-sensitive-u.s.-air-force-data.ht

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170314-01	Ondracek & Company	CA	3/15/2017	Electronic	Business	Yes - Published #	1,791

On February 6, 2017, we learned that some clients had received notification letters from the IRS telling them that someone had filed or attempted to file a 2016 tax return. On February 17, 2017, the specialized forensic IT firm determined that hackers had gained unauthorized access to our system from a foreign IP address. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NY AG' Author:
Article Title: Ondracek & Company
Article URL: https://oag.ca.gov/system/files/Ondracek%20Version%201_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170313-07	Pennsylvania Department of Revenue	PA	3/10/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

The Pennsylvania Department of Revenue is warning residents of a new phishing scam, targeting human resource and payroll employees. Criminals disguise an e-mail to look like a message being sent from an organization executive. The e-mail requests a W-2 form for each employee in the organization. They can then use the information to commit a number of crimes, including identity theft.

Attribution 1 Publication: abc27.com Author:
Article Title: W-2 scam affects 1,300 Pennsylvania tax payers
Article URL: http://abc27.com/2017/03/10/w-2-scam-affects-1300-pennsylvania-tax-payers/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170313-06	Virginia Commonwealth University Health System	VA	3/13/2017	Electronic	Medical/Healthcare	Yes - Published #	2,700

For the past three years, the electronic medical records of patients of Virginia Commonwealth University Health System have been inappropriately accessed by employees of physician groups.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Virginia Commonwealth University Health System Discovers 3-Year HIPAA Breach
Article URL: http://www.hipaajournal.com/virginia-commonwealth-university-health-system-discovers-3-year-hipaa-breach-8724/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170313-05	Health Texas Provider Network / Dental Heart Group	TX	3/10/2017	Electronic	Medical/Healthcare	Yes - Published #	22,562

On January 11, 2017, we learned that an external computer hard drive was stolen from the Clinic on or about December 29, 2016. The health information contained on the external hard drive may have included certain demographic information (such as your name, date of birth, address and phone number}, «Ciientoef1(driver's license number, Social Security number,)>> medical record number, clinic account number, insurance provider's name, insurance group and/or policynumbers, physician's name and clinical information (including diagnosis / conditions, lab test results and medications) related to medical care you received at the Clinic between 2009 and 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / hhs.gov / NY AG's offic Author:
Article Title: Health Texas Provider Network / Dental Heart Group
Article URL: https://dojmt.gov/wp-content/uploads/HealthTexas-Provider-Network-Denton-Heart-Group.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170313-04	**Hutchinson and Bloodgood LLP**	CA	3/13/2017	Electronic	Business	Yes - Published #	**25,558**

On December 21, 2016, we learned that a targeted “spear phishing” email was sent to employees of multiple CPA firms, including a Hutchinson and Bloodgood LLP employee. Based on our investigation, potentially accessible documents contained information, that may have included yourname, address and/or social security number. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / VT AG's office / NH AG' Author:
Article Title: Hutchinson and Bloodgood LLP
Article URL: https://oag.ca.gov/system/files/Notice_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170313-03	**Memphis VA Medical Center**	TN	3/1/2017	Paper Data	Government/Military	Yes - Published #	**687**

Memphis VA Medical Center TN Healthcare Provider 687 03/01/2017 Unauthorized Access/Disclosure Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170313-02	**CVS Health**	RI	3/8/2017	Paper Data	Medical/Healthcare	Yes - Published #	**724**

CVS Health RI Healthcare Provider 724 03/08/2017 Theft Paper/Films

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
ITRC20170313-01	**BJC Healthcare / Raising St. Louis**	MO	3/9/2017	Electronic	Medical/Healthcare	Yes - Published #	**644**

BJC Raising St. Louis staff discovered on January 9, 2017, that files containing enrollment and visit information for Raising St. Louis program participants were emailed between service providers in an unsecured manner between January 17, 2014, and January 9, 2017. The enrollment information included the participant’s name, address, telephone number, date of birth, date of visit, nursing notes and information related to medication and vaccinations. The email did NOT contain medical information such as diagnosis, tests, results, treatment or hospitalization, or financial data.

Attribution 1 Publication: hhs.gov / bjc.org / hipaajournal.com Author:
Article Title: BJC HealthCare Raising St. Louis Notifies Participants of Unencrypted Emails
Article URL: https://www.bjc.org/About-Us/Newsroom/BJC-News/ArtMID/897/ArticleID/2647/BJC-HealthCare-Raising-St-Louis-Notifi

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-18	**St. Francis Animal Hospital**	NV	3/9/2017	Paper Data	Business	Yes - Unknown #	**Unknown**

A large bag with files including names, addresses, and social security numbers was found left in a bag on a sidewalk near Charleston and Eastern. We found dozens of files from the early 2000's of pets from the St. Francis Animal Hospital. Each had the owners' names, phone numbers, addresses, and social security numbers.

Attribution 1 Publication: databreaches.net / ktnv.com Author:
Article Title: Personal information found in files dumped on sidewalk
Article URL: http://www.ktnv.com/news/personal-information-found-in-files-dumped-on-sidewalk

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-17	David Barton Gym (Club Ventures)	NY	3/10/2017	Paper Data	Business	Yes - Unknown #	Unknown

Paperwork containing the personal information of clients at a shuttered David Barton Gym in downtown Manhattan was found strewn across the heavily-trafficked streets in the area Thursday. News 4 cameras exclusively captured photocopies of identification cards, passports and visa information that had apparently been submitted with gym waivers for the luxury fitness chain.

Attribution 1 Publication: databreaches.net / nbcnewyork.com Author:
Article Title: Clients' Personal Info Exposed in Trashed Documents Near Shuttered David Barton Gym
Article URL: While our investigation is ongoing, we have evidence that your payroll information may have been accessed. Informati

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-16	VT Group	VA	3/3/2017	Electronic	Business	Yes - Published #	7,359

On October 4, 2016, VT Group was notified by the FBI that its network may have been subject to access by an unknown third party. While our investigation is ongoing, we have evidence that your payroll information may have been accessed. Information potentially affected includes your name, address, Social Security number, and direct deposit banking information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / ME A Author:
Article Title: VT Group
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/vt-group-20170303.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-15	Sallie Mae	DE	3/1/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

On October 28, 2016, a third party, not affiliated with Sallie Mae, obtained the following information about the affected New Hampshire resident: name, address, and social security number.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Sallie Mae
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/sallie-mae-20170301.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-14	RC Andersen Construction & Consulting, LLC	NJ	2/16/2017	Electronic	Business	Yes - Unknown #	Unknown

On January 26, 2017, the Company discovered that an employee's e-mail account had been criminally hacked. RC Andersen immediately commenced an investigation. While the investigation revealed that the hacker had misused the hacked e-mail account to send fraudulent e-mail, the investigation found no evidence that the hacker had accessed or acquired any personal information contained in the account. However, the Company cannot conclusively ruleout the possibility that personal information was unlawfully acquired.

Attribution 1 Publication: NH AG's office / CT AG's office Author:
Article Title: RC Andersen Construction & Consulting, LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/rcanderson-20170216.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-13	Roxy Trading / Chimes	CA	2/28/2017	Electronic	Business	Yes - Published #	443

Specifically, on January 22, 2017, a hacker gained access to our server and installed a form of "malware" known as "ransomware" to block access to our files. Among the files on the server that was hacked was a password-protected file with customer payment information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: Roxy Trading / Chimes
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/roxy-trading-20170228.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-12	Principal Financial Group	IA	2/27/2017	Electronic	Banking/Credit/Financial	Yes - Published #	1,094

The purpose for our letter is to notify you that your personal information was included in a January 2017 Contribution Report, which was sent to an incorrect plan sponsor on February 7, 2017. The 2017 Contribution Report contained your personal information, including your name and social security number. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Principal Financial Group
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/principal-financial-20170227.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-11	Kettle Cuisine	MA	2/7/2017	Electronic	Business	Yes - Published #	351

On Thursday, February 2, 2017, a Kettle Cuisine employee received an email requesting copies of our 2016 IRS Forms W-2 and W-3 . The email appeared to originate from Liam McClennon, Kettle Cuisine's CEO. The employee sent a reply email containing a Dropbox link to the 2016 IRS Forms W-2 and W-3. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: Kettle Cuisine
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/kettle-cuisine-20170207.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-10	Dawson Technical	TN	2/10/2017	Electronic	Business	Yes - Published #	500

On February 8, 2017, Dawson was the victim of an email phishing scam known as a W -2 Phishing Scam. The information obtained included employees' 2016 W-2 Forms that contained employees' social security numbers in electronic form.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Dawson
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280167.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-09	PCA Skin	AZ	2/28/2017	Electronic	Business	Yes - Unknown #	Unknown

I am writing to notify you that on February 22,2017, PCA Skin determined that it had been the victim of an email phlshing scheme that occurred earlier that same day, which resulted in the disclosure of certain 2016 employee W-2 forms.

Attribution 1 Publication: NH AG's office / MD AG's office / CT AG Author:
Article Title: PCA Skin
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/pca-skin-20170228.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-08	ProScan Imaging, LLC	OH	3/2/2017	Electronic	Medical/Healthcare	Yes - Published #	501

On February 24, 2017, we learned that one of our employees received a phishing email designed to appear as if it came from one of our Senior Executives. As a result of this phishing incident, we learned that an unauthorized individual may have obtained IRS Form W-2s for the 2016 employment year for some of our employees. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / CT AG's office / NY AG' Author:
Article Title: ProScan Imaging, LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/proscan-imaging-20170302.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-07	Joseph-Beth / Booksellers Enterprises LLC	OH	2/24/2017	Electronic	Business	Yes - Published #	483

On February 14, 2017, Booksellers Enterprises LLC (Joseph-Beth) learned that it was the victim of an e-mail phishing scam. As a result of this scam, an unknown individual fraudulently obtained copies of a number of Joseph-Beth employees and former employees personal data. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Joseph-Beth / Booksellers Enterprises LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/joseph-beth-20170224.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-06	Redington-Fairview General Hospital	ME	3/10/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

Patients who have previously received medical services at Redington-Fairview General Hospital in Skowhegan, Maine have been targeted with a new telephone phishing scam. The criminals behind the phishing scam are attempting to get patients to reveal sensitive financial information and credit card numbers over the telephone by impersonating the hospital.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Redington-Fairview General Hospital
Article URL: http://www.hipaajournal.com/redington-fairview-general-hospital-targeted-with-new-telephone-phishing-scam-8722/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-05	Ilovekickboxing.com (ILKB)	NY	3/9/2017	Electronic	Business	Yes - Published #	26,362

As a customer of ILKB, we want to inform you of a security concern that has recently arisen. On or about December 23, 2016, our third-party cybersecurity team reasonably determined that ILKB was the target of a sophisticated cyber-attack. As a result of our investigation, it appears that your private information may have been accessed by unauthorized persons during the first week of October 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NH AG's office / NY AG' Author:
Article Title: Ilovekickboxing.com
Article URL: https://dojmt.gov/wp-content/uploads/ILKB-Inc..pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-04	Maxim Capital Enterprises	NY	3/7/2017	Electronic	Business	Yes - Unknown #	Unknown

Credentials assigned to Maxim capital Enterprises, Inc. were used without authorization to access credit information from a consumer Information provider. This incident Involved Information typically found In a consumer report such as your name and address and one or more of the following: Social Security number, date of birth, or account numbers.

Attribution 1 Publication: MT AG's office / NH AG's office / NY AG' Author:
Article Title: Maxim Capital Enterprises
Article URL: https://dojmt.gov/wp-content/uploads/Maxim-Capital-Enterprises-Inc..pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-03	Wall Titus	FL	3/10/2017	Electronic	Business	Yes - Published #	1,442

We have recently learned that between December 20, 2016 and December 27, 2016 our computer system was compromised by an outside attacker who was able to gain access to our tax software. While we do not believe that any fraudulent tax returns were filed using our tax software, our investigation indicates that the unauthorized person did have access to the data in our software during this time. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / SC AG's office / NY AG' Author:
Article Title: Wall Titus
Article URL: https://dojmt.gov/wp-content/uploads/Wall-Titus-LLC.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-02	**Tarleton Medical**	CA	3/10/2017	Electronic	Medical/Healthcare	Yes - Published #	**3,929**

On January 6, 2017, TM learned of a data security incident that may have affected personal information contained in your medical records.On February 2, 2017, the digital forensics firm confirmed that TM's computer systems were accessed without authorization and indicated that patient records may have been accessed as well. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / ME AG's office / NY AG Author:
Article Title: Tarleton Medical
Article URL: https://oag.ca.gov/system/files/Tarleton%20-%20Employee%20Notification%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170310-01	**Verifone**	CA	3/9/2017	Electronic	Business	Yes - Published #	**232**

Credit and debit card payments giant Verifone [NYSE: PAY] is investigating a breach of its internal computer networks that appears to have impacted a number of companies running its point-of-sale solutions, according to sources. (Exposure number per NY AG's office / notification from Discover)

Attribution 1 Publication: krebsonsecurity.com / NY AG's office Author:
Article Title: Payments Giant Verifone Investigating Breach
Article URL: https://krebsonsecurity.com/2017/03/payments-giant-verifone-investigating-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170308-04	**Ohio Department of Rehabilitation and**	OH	3/8/2017	Electronic	Government/Military	Yes - Published #	**2,000**

The Ohio Department of Rehabilitation and Corrections mistakenly released the Social Security numbers of more than 2,000 inmates at the Chillicothe Correctional Institution to a convicted identity thief from Mansfield as part of a public records request.

Attribution 1 Publication: databreaches.net / mansfieldnewsjourna Author:
Article Title: Inmates' personal info mistakenly released to ID thief
Article URL: http://www.mansfieldnewsjournal.com/story/news/crime/2017/03/07/exclusive-inmates-ssns-mistakenly-released-ident

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170308-03	**Saliba's Extended Care Pharmacy**	AZ	3/8/2017	Electronic	Medical/Healthcare	Yes - Published #	**6,599**

On January 16, 2017, Saliba's Pharmacy discovered that on January 12, 2017, a copy of the December 2016 patient invoices was inadvertently emailed, via Saliba's Pharmacy's encrypted email platform, and thereafter opened by three other Saliba's Pharmacy patients or their Personal Representatives.

Attribution 1 Publication: hhs.gov / databreaches.net / hipaajourna Author:
Article Title: Saliba's Extended Care Pharmacy notifies more than 6,500 patients after email error
Article URL: https://www.databreaches.net/salibas-extended-care-pharmacy-notifies-more-than-6500-patients-after-email-error/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170308-02	**University of Georgia**	GA	3/8/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

What appears to be a combination list from various databases related to the University of Georgia appeared on a public paste site yesterday. The data, more than 4,800 records, consists of what appears to former and current students' and staff's email addresses and passwords, in some cases with usernames and IP addresses. For some records, the passwords are in plain text, while for others, they are encrypted. Some of the records appear to include date of birth, and some of the records appeared to have time stamps.

Attribution 1 Publication: databreaches.net Author:
Article Title: University of Georgia student and employee data found in data dump
Article URL: https://www.databreaches.net/university-of-georgia-student-and-employee-data-found-in-data-dump/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170308-01	**Friedman & Perry, CPAs**	CA	3/9/2017	Electronic	Business	Yes - Published #	**3,939**

On February 6, 2017, we learned that some clients had received notification letters from either the IRS or the FTB, regarding an attempted filing of their 2016 tax returns. On February 16, 2017, the specialized forensic IT firm determined that hackers had gained unauthorized access to our system from a foreign IP address. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / ME AG Author:
Article Title: Friedman & Perry, CPAs
Article URL: https://oag.ca.gov/system/files/Friedman%20Notification%20Letter%201_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170307-06	**Onyx Graphics, Inc.**	UT	2/22/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On February 13, 2017, we discovered that an employee had been the target of a phishing attack from a falsified email that purported to be from a legitimate source and requested copies of employee W-2 records. The employee replied to the email with the requested documents.

Attribution 1 Publication: NH AG's office Author:
Article Title: Onyx Graphics, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/onyx-graphics-20170221.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170307-05	**HealthInfoNet**	ME	2/9/2017	Electronic	Medical/Healthcare	Yes - Unknown #	**Unknown**

On January 24, 2017, a HealthInfoNet employee's email account was intentionally breached by someone seeking to gain access to the company's financial information. However, that was enough time for the potential retrieval of your personal information. The data accessed may have included personal information such as name, address, birth date, driver's license, social security number, and/or bank account number.

Attribution 1 Publication: NH AG's office / ME AG's office Author:
Article Title: HealthInfoNet
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/healthinfonet-20170214.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170307-04	**University of Idaho**	ID	3/6/2017	Electronic	Educational	Yes - Published #	**257**

On January 24, 2017, we detected that one of our accounts was being used to send phishing email. The email asked the employee to use their email account user name and password to sign-on to a website that appeared to be an Office 365 portal. The university immediately began an investigation and discovered that an unauthorized individual may have gained access to the employee's email, including the messages stored in the account. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170307-03	**Daytona State College #1**	FL	3/6/2017	Electronic	Educational	Yes - Published #	**26,603**

On February 19, I reported that I was finding 2016 W-2 tax statements for sale on the darknet. In that post, I noted that I was not identifying one Florida college I had contacted that day to alert them that at least one of their employees' W-2 statements was up for sale – and that others might be, too. Their CISO contacted me the next morning and began an investigation. (Exposure number per NY AG's office)

Attribution 1 Publication: databreaches.net / WFTV.com / NY AG' Author:
Article Title: Daytona State College notifies staff of potential W-2 incident
Article URL: https://www.databreaches.net/daytona-state-college-notifies-staff-of-potential-w-2-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170307-02	**Sunnyside Unified School District**	AZ	3/6/2017	Electronic	Educational	Yes - Published #	**599**

A pretty big mistake had Tucson's second largest school district scrambling to make sure its employees won't be hurt. Personal employee information was accidentally emailed to every Sunnyside Unified School District employee.

Attribution 1 Publication: databreaches.net / tucsonnewsnow.com Author:
Article Title: Sunnyside School District accidentally releases employees' personal information
Article URL: http://www.tucsonnewsnow.com/story/34679245/sunnyside-school-district-accidentally-releases-employees-personal-i

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170307-01	**Rhode Island Department of Human Services**	RI	3/6/2017	Paper Data	Government/Military	Yes - Published #	**1,100**

A new glitch in the computer system at Rhode Island's Department of Human Services resulted in more than 1,000 people receiving tax forms with the wrong information, putting their personal information at risk, state officials said Monday.

Attribution 1 Publication: databreaches.net / turnto10.com Author:
Article Title: DHS glitch results in tax form mistake
Article URL: http://turnto10.com/i-team/nbc-10-i-team-dhs-glitch-results-in-tax-form-mistake

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170306-06	**Retina Specialists (Robert E. Torti, MD)**	TX	2/17/2017	Paper Data	Medical/Healthcare	Yes - Published #	**887**

Robert E Torti, MD, PA dba Retina Specialists TX Healthcare Provider 887 02/17/2017 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Retina Specialists (Robert E. Torti, MD)
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=304DF04B09FB4F459F9113D48D3AF1FB

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170306-05	**VisionQuest Eyecare**	IN	3/2/2017	Electronic	Medical/Healthcare	Yes - Published #	**85,995**

Indiana-based VisionQuest Eyecare announced on its website that it discovered a cyber attack on its network on January 22, 2017. Information that was potentially compromised included patient names, addresses, phone numbers, dates of birth, Social Security numbers, health or vision insurance information, medical claims data and clinical information (Private Health Information), according to VisionQuest.

Attribution 1 Publication: hhs.gov / healthitsecurity. Author:
Article Title: VisionQuest Eyecare
Article URL: http://healthitsecurity.com/news/healthcare-hacking-leading-cause-for-2017-incidents

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170306-04	**Sharp Healthcare**	CA	3/3/2017	Electronic	Medical/Healthcare	Yes - Published #	**750**

The personal health information of more than 750 outpatients at Sharp Healthcare might have been compromised because of a computer theft, the San Diego-based medical care provider announced Friday.

Attribution 1 Publication: timesofsandiego.com / hipaajournal.com Author:
Article Title: Data of 750 Patients Compromised by Computer Theft at Sharp Healthcare
Article URL: http://timesofsandiego.com/crime/2017/03/03/data-of-750-patients-breached-in-computer-theft-at-sharp-healthcare/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170306-03	Alabama State Port Authority	AL	3/6/2017	Electronic	Government/Military	Yes - Published #	780

According to ASPA Vice President of Marketing Judith Adams, the organization was the victim of a spear phishing attack on Feb. 21 that targeted an employee with access to W-2 information for ASPA's employees and retirees — compromising the information of 780 individuals. The employee targeted at ASPA received an email appearing to be from CEO Jimmy Lyons, though it was in fact sent from an unknown external source. Purporting to be Lyons, the sender requested copies of W-2s for all ASPA employees, and according to Adams, "the employee fell for it, and that information was mistakenly released."

Attribution 1 Publication: databreaches.net / lagniappemobile.com Author:
Article Title: Port employees personal data released in 'cyber event'
Article URL: http://lagniappemobile.com/port-employees-personal-data-released-cyber-event/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170306-02	Glastonbury School District	CT	3/4/2017	Electronic	Educational	Yes - Published #	1,641

A phishing scandal has hit another Connecticut school district. Glastonbury school's superintendent said the district became victim of the W-2 phishing scam that has impacted other districts in the country and Groton. (Exposure number per NY AG's office)

Attribution 1 Publication: nbcconnecticut.com / NH AG's office / N Author:
Article Title: Glastonbury Schools Phishing Scandals Impacts 1,600 Workers
Article URL: http://www.nbcconnecticut.com/news/local/Glastonbury-Schools-Phishing-Scandals-Impacts-1600-Workers-41537489

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170306-01	Weidenhammer	PA	3/6/2017	Electronic	Business	Yes - Published #	180

Weidenhammer, which has several locations in Pennsylvania including Hanover Township, discovered last Thursday that it had suffered a "spear-phishing attack" that resulted in the theft of employees' W-2 tax information, company President John P. Weidenhammer confirmed Monday when I investigated an anonymous tip to The Morning Call.

Attribution 1 Publication: mcall.com Author:
Article Title: Company with Lehigh Valley offices loses employees' W-2 info. in phishing scam
Article URL: http://www.mcall.com/news/local/watchdog/mc-weidenhammer-data-breach-phishing-scam-watchdog-20170306-colu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-14	Genocea	MA	2/10/2017	Electronic	Business	Yes - Unknown #	Unknown

As you know, on February 1, 2017, one of our employees emailed W-2 information in response to what they later learned was a fraudulent email purporting to be from our CEO. In fact, the email was a phishing email that came from an external email address.

Attribution 1 Publication: NH AG's office Author:
Article Title: Genocea
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/genocea-20170210.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-13	Fresh Formats LLC	MA	2/22/2017	Electronic	Business	Yes - Published #	581

On or about November 10, 2016, our Information Technology Department detected malware on a Fresh Formats HR associate's computer. This associate had a file on her computer containing personal information of Fresh Formats associates. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MA OCABR / MD AG's Author:
Article Title: Fresh Formats LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/fresh-formats-20170222.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-12	Leo Edwards, Jr. MD	TX	2/28/2017	Electronic	Medical/Healthcare	Yes - Published #	19,564

On December 30, 2016, Or. Edwards discovered that an attacker may have gained access to his computer network in late November / December 2016. The network stored certain of his patients' personal information, including patients' names, addresses, dates of birth and, in some instances, Social Security numbers, diagnoses, lists of medications and health insurance information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / hhs.gov / MD AG's offic Author:
Article Title: Leo Edwards, Jr. MD
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/leo-edwards-20170228.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-11	Equian, LLC (Feb)	IN	2/27/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 17,2017, Equian discovered that on January 20,2017, an unauthorized third party may have received access to 20 I 6 W -2 tax forms of current and former Equian employees through a phishing email scam.

Attribution 1 Publication: NH AG's office / ME AG's office Author:
Article Title: Equian, LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/equian-20170227.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-10	Bentley University	MA	2/21/2017	Electronic	Educational	Yes - Unknown #	Unknown

On January 23, 2017, we learned that direct deposit account changes had been made for certain employees. Through our investigation, we learned that a targeted phishing email message had been sent to certain Bentley University employees. The attacker was able to use the login credentials that you provided via the phishing email to access and or view certain information in your Workday account. This information included your bank account number, bank routing information and Social Security number.

Attribution 1 Publication: NH AG's office / ME AG's office / CT AG' Author:
Article Title: Bentley University
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/bentley-university-20170221.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-09	Carla Cross, LLC	NM	3/3/2017	Electronic	Business	Yes - Published #	242

On February 14, 2017, I became aware that Carla Cross LLC had been the victim of a cyber intrusion by which an unknown third party was able to access my email address list. No evidence exists that anything other than the address list was accessed. However, in the event that some old emails may have been exposed, I am alerting you in case you ever sent me emails which contained your personal information. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / NY AG's office Author:
Article Title: Carla Cross, LLC
Article URL: https://dojmt.gov/wp-content/uploads/Carla-Cross-LLC.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-08	Tyler Independent School District	TX	3/3/2017	Electronic	Educational	Yes - Unknown #	Unknown

The Tyler Independent School District has issued a statement after employees fell victim to an email attack that seeks W-2 information. The district reportedly sent a letter to employees this week notifying them about W-2s that were sent outside the district. The 'attack' has been sweeping across the country with reports from several states. The e-mail requesting W-2 information is commonly sent to a district employee under the superintendent's name asking for W-2s for the district.

Attribution 1 Publication: databreaches.net / kltv.com Author:
Article Title: Tyler ISD issues statement after employee W-2 forms sent in 'email spoofing attack'
Article URL: http://www.kltv.com/story/34658970/sources-tyler-isd-employee-w-2-forms-sent-to-phishing-e-mail

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-07	MAM Software	PA	2/14/2017	Electronic	Business	Yes - Published #	81

On February 7, 2017, an employee of MAM Software, Inc. ("MAM") received a targeted fraudulent email requesting copies of W-2 forms for certain current and former personnel of MAM. The employee responded with PDF attachments of W-2s of approximately 81 individuals, of which 3 are residents of New Hampshire. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: MAM Software
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/mam-20170214.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-06	Lowe's	NC	3/3/2017	Electronic	Business	Yes - Unknown #	Unknown

Personal information connected to hundreds of Lowe's customers has been compromised. The breach is connected to a fax machine in Vancouver, Canada. A spokesperson from the company that owns the machine does not want to be identified, but said they have received more than 250 pages of customer order information in recent days.

Attribution 1 Publication: wsoctv.com / dataprivacy.net Author:
Article Title: Hundreds of Lowe's customers' personal information compromised
Article URL: http://www.wsoctv.com/news/local/hundreds-of-lowes-customers-personal-information-compromised/499082899

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-05	Center for Election Systems at Kennesaw State Univeristy	GA	3/3/2017	Electronic	Educational	Yes - Unknown #	Unknown

The Federal Bureau of Investigation is investigating an alleged data breach in Georgia at the Center for Election Systems at Kennesaw State University, The Atlanta Journal-Constitution has learned. The situation is still developing, although the Secretary of State's Office said Friday that the investigation is not related to its own network and is not a breach of its database containing the personal information on Georgia's 6.6 million registered voters.

Attribution 1 Publication: ajc.com Author:
Article Title: FBI investigating alleged breach in Georgia at KSU's elections center
Article URL: http://www.ajc.com/news/state--regional-govt--politics/fbi-investigating-alleged-breach-georgia-ksu-elections-center/c

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-04	Office of Syed Ahmed, MD, PA	TX	2/23/2017	Paper Data	Medical/Healthcare	Yes - Published #	79,930

Syed Ahmed, MD PA TX Healthcare Provider 500 02/23/2017 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Syed Ahmed, MD, PA
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-03	Abbott Northwestern Hospital / Minneapolis Heart Institute (	MN	2/23/2017	Paper Data	Medical/Healthcare	Yes - Published #	776

A member of a cleaning crew at the Minneapolis Heart Institute at Abbott Northwestern Hospital accidentally disposed of documents containing PHI with regular trash...a member of the cleaning team was discovered to have emptied a trash container from a physician's private office before documents could be securely shredded.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Abbott Northwestern Hospital / Minneapolis Heart Institute
Article URL: http://www.hipaajournal.com/improper-disposal-of-phi-discovered-by-minneapolis-heart-institute-8717/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-02	Groton Public Schools	CT	3/2/2017	Electronic	Educational	Yes - Published #	1,300

Groton Town Police are investigating after officials with the Groton Public Schools contacted them Thursday morning about a possible data breach. The investigation is in its preliminary stages, but evidence suggests the information was provided through a “Phishing” scam.

Attribution 1 Publication: connecticut.cbslocal.com /usnews.com / Author:
Article Title: Data Breach Being Investigated
Article URL: http://connecticut.cbslocal.com/2017/03/02/data-breach-being-investigated/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170303-01	Lake Kennedy McCulloch CPAs	WA	2/26/2017	Electronic	Business	Yes - Unknown #	Unknown

After a preliminary investigation, we discovered that perpetrators had illegally hacked into our system, and accessed 2015 tax return information for a number of our individual tax clients. Using this information, we believe they fraudulently filed some 2016 returns for the purpose of obtaining tax refunds.

Attribution 1 Publication: San Juan Islander / MT AG's office / NY Author:
Article Title: Data breach at local firm results in fraudulent tax returns
Article URL: http://sanjuanislander.com/news-articles/business-and-economy/24192/data-breach-at-local-firm-results-in-fraudulent-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-11	Ambassador Title Service	NE	2/28/2017	Electronic	Business	Yes - Unknown #	Unknown

On December 25, 2016, we learned that a possible data security incident may have impacted documents stored on our system. Unfortunately, on January 14, 2017, we learned that documents related to your home purchase or refinancing may have been impacted. These documents may have contained personal information about you, including your name, Social Security number, financial account information, and other transaction-related information.

Attribution 1 Publication: MT AG's office / NH AG's office / VT AG' Author:
Article Title: Ambassador Title Service
Article URL: https://dojmt.gov/wp-content/uploads/Ambassador-Title-Service_RTS-Title-Escrow_DRI-Title-Escrow.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-10	Millennium Solutions, Inc.	TX	2/28/2017	Paper Data	Business	Yes - Unknown #	Unknown

A viewer notified CHANNEL 5 NEWS he found stacks of folders filled with information of people from the Rio Grande Valley. Among the trash were copies of people’s driver’s license and Social Security cards attached to job applications.

Attribution 1 Publication: databreaches.net / KRGV.com Author:
Article Title: Inactive Company’s Applicant Personal Information Found in Dumpster
Article URL: http://www.krgv.com/story/34629951/inactive-companys-applicant-personal-information-found-in-dumpster

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-09	Aptos, Inc. (multiple retail stores)	GA	2/28/2017	Electronic	Business	Yes - Unknown #	Unknown

Aptos, Inc. provides e-commerce solutions for a number of online e-tailers. In November, 2016, Aptos discovered it had a malware breach from February, 2016 – December, 2016. At law enforcement’s request, they delayed notification to their clients, so we are first finding out about it now as the clients begin to disclose the breach to their customers.

Attribution 1 Publication: databreaches.net / WA AG's office / SC Author:
Article Title: Aptos malware breach affected 40 online retail stores
Article URL: https://www.databreaches.net/aptos-malware-breach-affected-40-online-retail-stores/

Attribution 2 Publication: VT AG's office / various sites Author:
Article Title: Aptos, Inc. - Affected Entities
Article URL: https://www.databreaches.net/aptos-malware-breach-affected-40-online-retail-stores/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-08	**Pasco Rentals, Inc.**	WA	2/24/2017	Electronic	Business	Yes - Published #	**6,300**

During the work of transferring records, on January 12, 2017, a USB drive containing a spreadsheet with a partial customer list and with some limited, personal information was lost or misplaced. The list included the name and driver's license number for some individuals, along with other customer information.

Attribution 1 Publication: WA AG's office Author:
Article Title: Pasco Rentals, Inc.
Article URL: http://agportal-s3bucket.s3.amazonaws.com/Breach%20Pasco%20Rentals%20Inc%202017-02-24.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-07	**Aero Air, LLC**	OR	2/2/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We are writing to inform you that as a result of a social engineering scam initiated by an unidentified individual, via e-mail, on January 11, 2017, some of your W-2 information may have been disclosed. The potentially compromised information may include your name, address, social security number and salary data.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-06	**Orange County Global Medical Center**	CA	2/8/2017	Electronic	Medical/Healthcare	Yes - Published #	**677**

In connection with preparing research regarding labor and delivery services provided to patients in 2016, on February 8, 2017, we discovered that an employee inadvertently emailed an Orange County Global Medical Center statistical report.

Attribution 1 Publication: CA AG's office / hhs.gov Author:
Article Title: Orange County Global Medical Center
Article URL: https://oag.ca.gov/system/files/Sample%20Notice_3.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-05	**University of California Santa Cruz**	CA	3/2/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

On January 13, 2017, two unencrypted laptops were stolen from the home of a University of California, Santa Cruz (UC Santa Cruz) researcher/instructor. The theft was discovered the same day and a police report was filed, but at this time no items have been recovered.

Attribution 1 Publication: CA AG's office Author:
Article Title: University of California Santa Cruz
Article URL: https://oag.ca.gov/system/files/UCSC_Notification_Letter_2017-01_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-04	**Stallcup & Associates CPAs**	CA	1/10/2017	Electronic	Business	Yes - Published #	**638**

On January 10, 2017, we became aware that some clients had received an email from our office that we did not send. Upon discovery of this fraudulent activity, we sent an email alerting you not to open the email. Per FOIL NY AG's office

Attribution 1 Publication: CA AG's office / NY AG's office Author:
Article Title: Stallcup & Associates CPAs
Article URL: https://oag.ca.gov/system/files/Stallcup%20Notification%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-03	**Allied Minds, LLC**	MA	2/27/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On or around February 13, 2017, an Allied Minds employee received, and complied with, an email appearing to come from another Allied Minds employee requesting the release of W-2 tax information for Allied Minds employees for the 2016 tax year.

Attribution 1 Publication: NH AG's office / MD AG's office / ME A Author:
Article Title: Allied Minds, LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/allied-minds-20170224.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-02	Yukon Public Schools	OK	3/2/2017	Electronic	Educational	Yes - Unknown #	Unknown

The school alerted employees on March 1, W-2 information was stolen.
The HR department fell victim to a phishing scam requesting the W-2 information for all school employees, Superintendent Dr. Jason Simeroth said. He said the email look like it was sent from him.

Attribution 1 Publication: pkcfox.com Author:
Article Title: Yukon Public Schools hit with data breach
Article URL: http://okcfox.com/news/local/yukon-public-schools-hit-with-data-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170302-01	MetWest Terra Hospitality	WY	2/23/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 9, 2017, we leamed that a targeted "spear phishing" email message had been sent to a MetWest Terra Hospitality employee.

Attribution 1 Publication: CA AG's office Author:
Article Title: MetWest Terra Hospitality
Article URL: https://oag.ca.gov/system/files/redacted%20letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170301-05	Northeast Ohio Regional Sewer District	OH	3/1/2017	Electronic	Business	Yes - Published #	897

The Northeast Ohio Regional Sewer District has accidentally released W-2 information for all of the district's nearly 900 employees. In a "phishing" scheme, someone posed online as sewer district Chief Executive Officer Kyle Dreyfuss-Wells and requested copies of all the employees W-2 tax forms, Dreyfuss-Wells said. (Exposure number per NY AG's office)

Attribution 1 Publication: databreaches.net / cleveland.com / NY Author:
Article Title: Northeast Ohio Regional Sewer District releases employee tax info in phishing scheme
Article URL: http://www.cleveland.com/metro/index.ssf/2017/03/northeast_ohio_regional_sewer_2.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170301-04	Autoneum North America, Inc.	MI	3/1/2017	Electronic	Business	Yes - Published #	2,400

Autoneum North America Inc. said the data included 2016 W-2 salary and tax information as well as the current and former workers' names, addresses and Social Security numbers. Company spokeswoman Anahid Rickmann said it has been working with the FBI and IRS to investigate the breach and has offered its employees identity repair and credit monitoring services. She said the information was stolen "with criminal intent."

Attribution 1 Publication: databreaches.net / mcall.com Author:
Article Title: Car parts maker says scam got tax info for 2,400 workers
Article URL: http://www.mcall.com/business/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170301-03	ABNB Federal Credit Union	VA	1/24/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

An employee received an email from what appeared to be the employee's supervisor requesting copies of all W-2s for 2015 and 2016. The employee responded to the email and provided the W-2s for 2015, which also included certain information to be reported on Form 1 095-C.

Attribution 1 Publication: databreaches.net / MD AG's office Author:
Article Title: ABNB Federal Credit Union
Article URL: https://www.databreaches.net/wp-content/uploads/ABNBFCU.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170301-02	**Tata Access Floors**	MD	1/13/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On Wed rnoming, an associate in the Human resources department received and email that appeared to have been sent from our company president requesting copies of his direct reports W2 tax forms from the years 2015 & 2016.

Attribution 1 Publication: databreaches.net / MD AG's office Author:
Article Title: Tata Access Floors
Article URL: https://www.databreaches.net/wp-content/uploads/Tate.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170301-01	**Wisenbaker Building Services**	AL	2/10/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We recently discovered that our company was the victim of an email spoofing attack today, February 10, 2017, by an individual pretending to be our owner. A request was made from what appeared to be a legitimate Wisenbaker email address for all 2016 Wisenbaker employee W-2 information.

Attribution 1 Publication: MT AG's office Author:
Article Title: Wisenbaker Building Services
Article URL: https://dojmt.gov/wp-content/uploads/Wisenbaker-Builder-Services.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-24	**TrueNet Communications**	FL	1/26/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Specifically, a third party obtained unauthorized access to some of our employee information through a phishing-type attack in which an outside party posing as a TrueNet employee convinced another employee to provide a file containing employee information.

Attribution 1 Publication: databreaches.net / MD AG's office Author:
Article Title: TrueNet Communications
Article URL: https://www.databreaches.net/wp-content/uploads/TrueNetComm.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-23	**2020 On-Site Optometry**	MA	2/13/2017	Electronic	Medical/Healthcare	Yes - Published #	**15,400**

2020 On-Site Optometry MA Business Associate 15400 02/13/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: 2020 On-Site Optometry
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-22	**Chadron Community Hospital & Health Services**	NE	2/19/2017	Electronic	Medical/Healthcare	Yes - Published #	**702**

Last month, Chadron Community Hospital and Health Services in Nevada discovered that a rogue employee had been accessing ePHI without any legitimate work reason for doing so. What makes this incident stand out, is how long access had been allowed to continue before it was discovered.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: Chadron Community Hospital & Health Services
Article URL: http://www.hipaajournal.com/healthcare-employee-accessed-ephi-without-authorization-5-years-8716/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-21	New York Life Insurance Company	NY	1/30/2017	Electronic	Business	Yes - Published #	2,367

Recently, we learned that an individual placed at New York Life by a temporary employment agency used a fake identity to hide a criminal background. The individual worked at New York Life for the month of December 2016. While temporarily employed at New York Life, this individual had access to personal information, including the name, Social Security Number, date of birth, and address of 10 New Hampshire residents. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: New York Life
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/new-york-lfe-20170130.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-20	John Deere Financial	WI	2/27/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

We are contacting you to notify you of a recent data security incident that occurred on January 24, 2017 involving personal information about you. This incident involved a misdirected email sent by John Deere Financial that included personal information such as your name, Social Security number, and John Deere Financial account number and balance information.

Attribution 1 Publication: MT AG's office / WI AG's office / ME AG' Author:
Article Title: John Deere Financial
Article URL: https://dojmt.gov/wp-content/uploads/John-Deere-Financial.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-18	U.S. Anti-Doping Agency	CO	2/24/2017	Electronic	Business	Yes - Unknown #	Unknown

On October 6, 2016, we also discovered that the documents released by Fancy Bears contained information that appeared to have come from the email address of a USADA employee. The information was related to therapeutic use exemptions (TUEs), and as such, we immediately launched an internal investigation and retained third-party forensic experts to assist in the investigation of the incident.

Attribution 1 Publication: MT AG's office / CT AG's office Author:
Article Title: U.S. Anti-Doping Agency
Article URL: https://dojmt.gov/wp-content/uploads/United-States-Anti-Doping-Agency.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-17	Benchmark	TX	2/24/2017	Electronic	Business	Yes - Unknown #	Unknown

After being alerted to a potential security incident at one of its managed properties, Benchmark initiated an investigation at that property and identified an unauthorized file designed to capture payment card information as it is routed through its payment processing system.

Attribution 1 Publication: VT AG's office / NH AG's office / MD AG' Author:
Article Title: Benchmark Notifies Customers of Payment Card Incident
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Benchmark%20SBN%20to%20Consumers.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-16	John D. Williamson, CPA	CA	2/9/2017	Electronic	Business	Yes - Published #	738

n the morning of February 10, 2017 I discovered that my car had been stolen sometime between the night of February 9, 2017 and that morning. Inside my trunk were two password protected laptop computers containing tax software for my personal tax clients. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / NY AG' Author:
Article Title: John D. Williamson, CPA
Article URL: https://oag.ca.gov/system/files/JWCPA%20-%20Notice%20of%20Data%20Event%20-%20Notice%20Only%201_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-14	Vanderbilt University Medical Center	TN	2/25/2017	Electronic	Medical/Healthcare	Yes - Published #	3,247

Vanderbilt University Medical Center officials say the hospital has had a security breach where two employees accessed medical records of more than 3,000 patients.

Attribution 1 Publication: databreaches.net / wkms.org / hipaajour Author:
Article Title: Vanderbilt University Medical Center Security Breach Affects 3,000 Patients, Officials Say
Article URL: http://wkms.org/post/vanderbilt-university-medical-center-security-breach-affects-3000-patients-officials-say

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-13	Chicago Public Schools	IL	2/25/2017	Electronic	Educational	Yes - Unknown #	Unknown

Confidential information about Chicago Public Schools students — including medical conditions and dates of birth — was kept on unsecured web documents that anyone could call up despite laws and CPS rules that are supposed to safeguard children's privacy. The breach also included special education students' names, identification numbers and other information that's supposed to be kept confidential but was viewable in payment records that were posted on CPS' website.

Attribution 1 Publication: databreaches.net / chicago.suntimes.co Author:
Article Title: CPS privacy breach bared confidential student information
Article URL: http://chicago.suntimes.com/news/cps-privacy-breach-bared-confidential-student-information/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-12	Downeast Credit Union	ME	2/27/2017	Electronic	Banking/Credit/Financial	Yes - Unknown #	Unknown

Customers of Downeast Credit Union in Belfast are being urged to check their accounts, after more than two dozen people reported hundreds of dollars were stolen from their accounts. Customers of Downeast Credit Union in Belfast are being urged to check their accounts, after more than two dozen people reported hundreds of dollars were stolen from their accounts.

Attribution 1 Publication: databreaches.net / WABI.com Author:
Article Title: ME: Belfast Police Warn of Security Breach at Credit Union
Article URL: https://www.databreaches.net/me-belfast-police-warn-of-security-breach-at-credit-union/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-11	Niagara-Wheatfield School District	NY	2/26/2017	Electronic	Educational	Yes - Unknown #	Unknown

Officials with the Niagara-Wheatfield School District are warning of a possible link between a recently used ticket sales platform and credit card fraud.

Attribution 1 Publication: databreaches.net / niagara-gazette.com Author:
Article Title: Niagara-Wheatfield warning of possible credit card fraud
Article URL: http://www.niagara-gazette.com/news/local_news/niagara-wheatfield-warning-of-possible-credit-card-fraud/article_a34

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-10	Veteran's Affairs	IL	2/27/2017	Electronic	Government/Military	Yes - Published #	724

A total of 724 patient's records were released by the former employee to an employee not involved in the medical care of those veterans. The VA's office of the Inspector General is aiding in the investigation of this alleged information leak.

Attribution 1 Publication: databreaches.net / altondailynews.com Author:
Article Title: Veteran's Affairs
Article URL: http://altondailynews.com/news/details.cfm?clientid=17&id=237811 - .WLW7TOQzWHI

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-09	**North Carolina Department of Health and Human Services**	NC	2/27/2017	Electronic	Government/Military	Yes - Published #	**12,731**

The state Department of Health and Human Services sent private patient information to adult care homes by unencrypted email last year. The security lapse involved 12,731 Medicaid patients living in adult care homes. On Nov. 30, an employee sent an unencrypted email that included patient names, Medicaid numbers, and the homes where the patients resided.

Attribution 1 Publication: databreaches.net / newsobserver.com / Author:
Article Title: NC health department exposed patient information in email
Article URL: http://www.newsobserver.com/news/politics-government/politics-columns-blogs/under-the-dome/article134607114.ht

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-08	**CloudPets (Spiral Toys)**	CA	2/27/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Troy Hunt reports that a misconfigured MongoDB installation resulted in audio files of children's and parents' conversations recorded by CloudPets being exposed in a Shodan search.

Attribution 1 Publication: databreaches.net Author:
Article Title: Data from connected CloudPets teddy bears leaked due to misconfigured database; 820,000 kids' files exposed
Article URL: https://www.databreaches.net/data-from-connected-cloudpets-teddy-bears-leaked-due-to-misconfigured-database-820

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-07	**Independent School District**	MO	2/27/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

The school district employees were alerted to the scam in an email sent last Thursday. In it, the business office says the "the names, social security numbers, addresses and earnings" of every employee was stolen in a phishing scam, where the crooks use fake emails or websites to steal person information.

Attribution 1 Publication: databreaches.net / kcur.org Author:
Article Title: Social Security Numbers Stolen From All Independence School Employees
Article URL: http://kcur.org/post/social-security-numbers-stolen-all-independence-school-employees - stream/0

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-06	**Redmond School District**	OR	2/27/2017	Electronic	Educational	Yes - Published #	**1,000**

According to the internal email, a scammer impersonating McIntosh requested via email W-2s for all employees, and received them Friday via email. The documents contain employees' names, social security numbers, mailing addresses, wages and tax-withholding information.

Attribution 1 Publication: databreaches.net / bendbulletin.com / O Author:
Article Title: More than 1,000 W-2s stolen from Redmond School District
Article URL: http://www.bendbulletin.com/localstate/5106585-151/more-than-1000-w-2s-stolen-from-redmond-school

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-05	**Vintage Realty Company**	LA	2/25/2017	Electronic	Business	Yes - Unknown #	**Unknown**

The email read, "In the last week, two Vintage employees received emails, appearing to be from a principal at Vintage, requesting W-2 information about vintage employees. A Vintage employee replied to one of the requests and attached Vintage's 2015 and 2016 W-2s for all employees.

Attribution 1 Publication: databreaches.net / shreveporttimes.com Author:
Article Title: Vintage Realty security breach impacts employees
Article URL: http://www.shreveporttimes.com/story/news/crime/2017/02/26/vintage-realty-security-breach-impacts-employees/98350

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-04	Beckett Air	OH	2/27/2017	Electronic	Business	Yes - Published #	200

North Ridgeville police report nearly 200 employees with Beckett Air have been victimized by a W-2 scam that has hit a growing number of Northeast Ohio businesses, cities and non-profit organizations.

Attribution 1 Publication: databreaches.net / newsnet5.com Author:
Article Title: North Ridgeville Beckett Air employees victimized by W-2 scam
Article URL: http://www.newsnet5.com/news/local-news/north-ridgeville-beckett-air-employees-victimized-by-w-2-scam

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-03	Accolade, Inc.	CA	1/23/2017	Electronic	Business	Yes - Published #	937

On Thursday, January 19, 2017, Accolade learned that it was a victim of a phishing scheme that included a targeted email, sent January 17, 2017, requesting employee W-2s. (Exposure number per NY AG's office)

Attribution 1 Publication: databreaches.net / MD AG's office / NY Author:
Article Title: Accolade, Inc.
Article URL: https://www.databreaches.net/wp-content/uploads/Accolade.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-02	Bentley Truck Services	PA	1/26/2017	Electronic	Business	Yes - Published #	Unknown

Bentley Truck Services, Inc. (“Bentley”) was the targeted victim of an email spoofing attack on January 24, 2017, by an individual pretending to be Bentley’s Owner.

Attribution 1 Publication: databreaches.net / MD AG's office Author:
Article Title: Bentley Truck Services
Article URL: https://www.databreaches.net/wp-content/uploads/BentleyTruckSvces.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170228-01	Pacific Biosciences of California, Inc.	CA	1/30/2017	Electronic	Business	Yes - Published #	454

On January 21, 2017, a Pacific Biosciences employee was tricked into disclosing employees’ W-2 information to an unauthorized individual as part of a phishing attack. (Exposure number per NY AG's office)

Attribution 1 Publication: databreaches.net / MD AG's office / NY Author:
Article Title: Pacific Biosciences of California, Inc.
Article URL: https://www.databreaches.net/wp-content/uploads/PacificBiosciences.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170227-05	Verato, Inc.	VA	1/30/2017	Electronic	Business	Yes - Unknown #	Unknown

On January 25, 2017, Verato was the target of a phishing email that resulted in the unauthorized acquisition by an unknown third party of employees' W-2 tax forms.

Attribution 1 Publication: databreaches.net / MD AG's office Author:
Article Title: Verato, Inc.
Article URL: https://www.databreaches.net/wp-content/uploads/Verato.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170227-04	TrustComm, Inc.	VA	1/12/2017	Electronic	Business	Yes - Unknown #	Unknown

In the afternoon of January 10, 2017, TrustComm determined that earlier that day, a criminal impersonating a senior Company official had requested and received Internal Revenue Service (IRS) W-2 forms, containing the personal information of a number of employees of the Company, including their Social Security numbers.

Attribution 1 Publication: databreaches.net / MD AG's office Author:
Article Title: TrustComm, Inc.
Article URL: https://www.databreaches.net/wp-content/uploads/TrustComm.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170227-03	Rod's Western Palace	OH	2/24/2017	Electronic	Business	Yes - Published #	34,255

After identifying suspicious activity within our e-commerce site on February 8, 2017, we immediately initiated an internal investigation and engaged external IT consultants to assist us. By February 10th, we identified the malicious code, permanently removed it from our site, and took additional steps to prevent a similar intrusion. Based on our investigation, the information potentially involved in this incident may have included your name, credit or debit card number, card expiration date and CW2/CVC2/CID/CVD (security code on the front or back of the card). (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / VT AG's office / NY AG' Author:
Article Title: Rod's Western Palace
Article URL: https://oag.ca.gov/system/files/Rod%27s%20Western%20Palace%20-%20CA%20Notification%20%286607474-2x7AB84

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170227-01	Roberts Hawaii, Inc.	HI	2/24/2017	Electronic	Business	Yes - Published #	30,180

The investigation determined that an unauthorized person gained access to the web server for robertshawaii.com and airportwaikikishuttle.com and installed code that was designed to copy information entered during the checkout process, including, name, address, email address, phone number, payment card number, expiration date and card security code. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / OR AG's office / Vt AG' Author:
Article Title: Roberts Hawaii, Inc.
Article URL: https://oag.ca.gov/system/files/NPC_Breach_C5920_CA_Sample_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-17	Tab Products Co., LLC	WI	2/15/2017	Electronic	Business	Yes - Published #	183

On February 7, 2017, TAB discovered that it had been the victim of an email phishing scam that Jed a TAB employee to inadvertently release to a third party certain 20161RS Form W-2, Wage and Tax Statements of TAB employees. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / WI AG's office / MD AG' Author:
Article Title: Tab Products Co., LLC
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/tab-20170210.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-16	West Virginia University Hospitals dba University	WV	2/24/2017	Electronic	Medical/Healthcare	Yes - Published #	7,445

More than 7,000 patients of WVU Medicine University Healthcare were notified of a breach of unsecured personal patient protected health information after discovering that an employee had accessed patient information without authorization.

Attribution 1 Publication: MD AG's office Author:
Article Title: West Virginia University Medicine University Healthcare DBA University HealthCare
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280199.pdf

Attribution 2 Publication: journal-news.net / hhs.gov / MD AG's offi Author:
Article Title: 7,445 patients notified of University Healthcare information breach
Article URL: http://www.journal-news.net/news/local-news/2017/02/7445-patients-notified-of-university-healthcare-information-brea

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-15	**Ysleta Independent School District**	TX	2/24/2017	Electronic	Educational	Yes - Published #	**1,700**

Confidential information belonging to Hanks High School students might have been compromised after a laptop containing transcripts of every student at the school was stolen. A Hanks counselor downloaded and saved transcripts of all 1,700 students onto a personal laptop as part of her job, but the laptop and other items were stolen from her home on Feb. 18. Transcripts contain students' birth dates, Social Security numbers, home addresses and parents' or guardians' names.

Attribution 1 Publication: elpasotimes.com Author:
Article Title: Laptop stolen; Hanks students at risk of ID theft
Article URL: http://www.elpasotimes.com/story/news/education/2017/02/24/laptop-stolen-hanks-students-risk-id-theft/98358928/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-14	**Amalgamated Sugar**	ID	2/24/2017	Electronic	Business	Yes - Published #	**2,858**

Management officials of The Amalgamated Sugar Company, LLC distributed letters to its employees Thursday, notifying them that the company suffered “a data breach that has resulted in the disclosure of employee personal information to an unauthorized personal outside of the business. “The breach was triggered through an e-mail scam known as a spear-fishing attack. Someone posing as our CEO and mimicking his company e-mail address sent an e-mail to a corporate office employee requesting copies of our employees’ W-2s.

Attribution 1 Publication: kivitv.com / Scmagazine.com Author:
Article Title: Amalgamated Sugar suffers cyber security breach; 2,858 workers' personal info stolen
Article URL: http://www.kivitv.com/news/amalgamated-sugar-suffers-cyber-security-breach-workers-personal-info-stolen-in-phishi

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-13	**Cloudflare**	CA	2/24/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Security firm Cloudflare disclosed late Thursday that a long-running bug in its security systems may have leaked information, including potentially personal information, from thousands of sites including Uber, Fitbit and OK Cupid.

Attribution 1 Publication: chicagotribune.com / WI AG's office Author:
Article Title: Major security flaw means you have to change your passwords again
Article URL: http://www.chicagotribune.com/bluesky/technology/ct-cloudflare-security-flaw-wp-bsi-20170224-story.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-12	**Roy & Bentas CPAs, PC**	NH	2/3/2017	Electronic	Business	Yes - Published #	**209**

The purpose of this letter is to inform you about a breach related to tax information held by Roy & Benta s CPA's , P.C. (R&B). On February 2, 2017, R&B discovered that a hacker had executed a sophisticated cyber attack to obtain access to R&B's ShareFile portal, and had downloaded from the portal personal tax information for a number of R&B's clients. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG'soffice / NH AG's office / NY AG' Author:
Article Title: Roy & Bentas CPAs, PC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Roy%20&%20Bentas%20CPAs,%20P.C%20SBN%20to

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-10	**Group Health Inc.**	NY	2/17/2017	Paper Data	Medical/Healthcare	Yes - Published #	**703**

Group Health Incorporated NY Health Plan 703 02/17/2017 Unauthorized Access/Disclosure Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-09	**Medical Information Management Systems, Inc.**	FL	2/9/2017	Electronic	Business	Yes - Published #	**11,707**

Medical Information Management Systems, LLC FL Business Associate 11707 02/09/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Medical Information Management Systems, 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
ITRC20170224-08	**New York City Department of Education**	NY	2/22/2017	Electronic	Government/Military	Yes - Published #	**439**

New York City's Department of Education accidentally sent out an email that had not just the names, but also the Social Security numbers of hundreds of employees.

Attribution 1 Publication: databreaches.net / abc7ny.com Author:
Article Title: Exclusive: DOE emails hundreds of teacher's assistants' social security numbers
Article URL: http://abc7ny.com/education/exclusive-doe-emails-hundreds-of-employee-social-security-numbers/1767721/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-07	**South Washington County School District**	MN	2/22/2017	Electronic	Educational	Yes - Published #	**478**

The South Washington County school district is tightening security after a high school student hacked into the district's server and took names, Social Security numbers and some addresses.

Attribution 1 Publication: databreaches.net / startribune.com Author:
Article Title: South Washington School District probes hacking by student
Article URL: http://www.startribune.com/south-washington-school-district-investigating-student-hacking-incident/414524663/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-06	**Abernathy Independent School District**	TX	2/22/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

Sensitive tax information belonging to employees of Abernathy Independent School District was leaked last week after the district was hit with a phishing scam. Superintendent Dr. Glen Teal, Ed.D. said employees' W-2 information was released in the breach. He said other district statewide and around the nation have also fallen victim.

Attribution 1 Publication: databreaches.net / everythinglubbock.co Author:
Article Title: Teacher Info Leaked in Security Breach at Abernathy ISD
Article URL: http://www.everythinglubbock.com/news/kamc-news/teacher-info-leaked-in-security-breach-at-abernathy-isd/66085506

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-05	**Civitas Media**	NC	2/23/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Civitas Media, the North Carolina-based parent company of The Times Leader, contacted law enforcement after an employee released federal W-2 forms to a person posing as a Civitas officer, according a letter from the company to its employees.

Attribution 1 Publication: databreaches.net / citizensvoice.com Author:
Article Title: Times Leader parent company contacts law enforcement after email scam involving tax forms
Article URL: http://citizensvoice.com/news/times-leader-parent-company-contacts-law-enforcement-after-email-scam-involving-tax-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-04	**Ellwood Thompson's Local Market**	VA	2/23/2017	Electronic	Business	Yes - Published #	**360**

Ellwood Thompson's Local Market employees' personal information was recently divulged in a phishing scam. According to a document sent to employees, about 360 current and former employees were impacted by the breach.

Attribution 1 Publication: databreaches.net / wric.com Author:
Article Title: Ellwood Thompson's security compromised in cyber scam
Article URL: http://wric.com/2017/02/23/ellwood-thompsons-employees-fall-victim-to-phishing-scam/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-03	North Carolina Symphony	NC	2/23/2017	Electronic	Business	Yes - Published #	262

According to a report filed with the North Carolina Attorney General's office, the Feb. 7 leak involved the mistaken release of W-2 tax information for 262 people, including symphony musicians, staff and contract employees. All but 20 of those affected are North Carolina residents.

Attribution 1 Publication: databreaches.net / newsobserver.com / Author:
Article Title: Phishing scam catches NC Symphony
Article URL: http://www.newsobserver.com/entertainment/music-news-reviews/on-the-beat-blog/article134525844.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-02	Coachella Music Festival (Goldenvoice)	CA	2/23/2017	Electronic	Business	Yes - Published #	27,000

An unidentified hacker calling himself Berkut is selling more than 950,000 user accounts for the Coachella music festival, including email addresses, user names and hashed passwords, calling the info a "complete database dump from this month," Motherboard reports. (Exposure number per NY AG's office)

Attribution 1 Publication: esecurityplanet.com / CA AG's office / N Author:
Article Title: Coachella Music Festival (Goldenvoice)
Article URL: http://www.esecurityplanet.com/hackers/950000-coachella-user-accounts-offered-for-sale-online.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170224-01	Logic Supply	VT	2/6/2017	Electronic	Business	Yes - Unknown #	Unknown

Yesterday, February 6th, we discovered unauthorized access to our website, which made some customer information vulnerable. However the attacker may have accessed, among other things: LogicSupply.com Username & Password, Customer (Company) names, Order information

Attribution 1 Publication: CA AG's office Author:
Article Title: Logic Supply
Article URL: https://oag.ca.gov/system/files/LS%20Notice%20of%20DB%20-%20US%202-7-17_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170223-09	Boulrice & Wood CPAs, PC	NY	2/10/2017	Electronic	Business	Yes - Published #	766

On Tuesday, January 31, 2017, Boulrice & Wood CPAs, PC ("Boulrice & Wood") received notification that fraudulent tax returns had been filed for certain individuals and businesses whose prior tax returns had been filed by Boulrice & Wood. After an investigation, we discovered unauthorized access to a tax program, utilized by our company, between January 7, 2017 and January 17, 2017. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / MD AG' Author:
Article Title: Boulrice & Wood CPAs, PC
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Boulrice%20and%20Wood%20CPAs%20SBN%20to%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170223-08	Art of Shaving	TX	2/15/2017	Electronic	Business	Yes - Unknown #	Unknown

On February 6, 2017, the supplier who operates a portion of our order processing system notified us that their systems had been breached. The breach occurred between February and December of 2016. Our records show that you made a non-standard order between November 2015 and December 2016.

Attribution 1 Publication: VT AG's office / MD AG's office / NY Author:
Article Title: Art of Shaving
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/The%20Art%20of%20Shaving%20SBN%20to%20Consu

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170223-07	Insperity	TX	2/17/2017	Electronic	Business	Yes - Unknown #	Unknown

We recently had a former client request a report for tax reporting purposes. In responding to this company, a report containing your name, social security number, and address was inadvertently emailed to the president and financial manager of that company on February 3, 2017.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170223-06	Gardiner & Appel Group	MD	2/16/2017	Electronic	Business	Yes - Published #	1,281

On or about January 16, 2017, Gardiner & Appel Group became the victim of a cyber attack by which an unknown third party was able to access Gardiner & Appel Group's computer network and some of its client's personal information. As a result, some of your personal information may have been exposed to others, including your first and last name, home address, social security number, and 2015 compensation data. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / MD AG' Author:
Article Title: Gardiner & Appel Group
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Gardiner%20&%20Appel%20Group,%20Inc.%20SBN%2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170223-05	LEAF Commercial Capital	CO	2/21/2017	Electronic	Business	Yes - Published #	327

On February 16, 2017, we learned that a targeted "spear phishing" email message had been sent to LEAF that same day. Believing the email to be legitimate, LEAF replied to the message on the day the email was received and attached 2016 Forms W2 for current and former employees, which included your name, address, Social Security Number, and earnings information. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / MD AG's office / NY AG' Author:
Article Title: LEAF Commercial Capital
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/LEAF%20Commercial%20Capital,%20Inc.%20SBN%20t

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170223-04	Arabella Advisors	DC	2/22/2017	Electronic	Business	Yes - Published #	553

On February 9, 2017, Arabella Advisors, LLC discovered that an unauthorized person had gained access to Arabella servers containing certain personal information. As a result of this incident, your name, address, date of birth, and social security number may have been potentially exposed to others. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / MD AG's office / ME AG Author:
Article Title: Arabella Advisors
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Arabella%20Advisors,%20LLC%20SBN%20to%20Cons

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170223-03	Cayan	MA	2/22/2017	Electronic	Business	Yes - Published #	331

We recently discovered that a security incident occurred involving your personal information. On or about February 9, 2017, an unauthorized individual acquired a copy of your 2016 W-2, Wage and Tax
Statement. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170223-02	**InterMountain Management, LLC**	LA	2/21/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We recently discovered that our company was the victim of an email spoofing attack on February 3, 2017, by an individual pretending to be the owner of our company. A request was made for all 2016 W-2 forms prepared by InterMountain. Unfortunately, copies of all 2016 W-2 forms prepared by InterMountain were provided before we discovered that the request was made from a fraudulent account.

Attribution 1 Publication: MT AG's office / VT AG's office / NH AG' Author:
Article Title: InterMountain Management, LLC
Article URL: https://dojmt.gov/wp-content/uploads/InterMountain-Management.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170223-01	**Viskase**	IL	2/22/2017	Electronic	Business	Yes - Published #	**590**

We have just learned that Viskase has become the victim of an email phishing incident that resulted in disclosure of the information on its hourly and non-exempt employees' 2015 IRS W-2 forms.

Attribution 1 Publication: databreaches.net / kait8,com Author:
Article Title: Phishing scam nets hundreds of Viskase employee IDs
Article URL: http://www.kait8.com/story/34576218/phishing-scam-nets-hundreds-of-viskase-employee-ids

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-34	**Walgreen Co.**	IL	2/3/2017	Paper Data	Medical/Healthcare	Yes - Published #	**4,500**

Walgreen Co. IL Healthcare Provider 4500 02/03/2017 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
ITRC20170222-33	**Bloom Physical Therapy, LLC dba Physicians Physical**	AZ	2/9/2017	Electronic	Medical/Healthcare	Yes - Published #	**500**

Bloom Physical Therapy, LLC dba Physicians Physical Therapy Service AZ Healthcare Provider 500 02/09/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Bloom Physical Therapy, LLC dba Physicians Physical Therapy Service
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-32	**Benesch, Friedlander, Coplan & Aronoff, LLP**	OH	2/10/2017	Paper Data	Business	Yes - Published #	**1,134**

Benesch, Friedlander, Coplan & Aronoff LLP OH Business Associate 1134 02/10/2017 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Benesch, Friedlander, Coplan & Aronoff, 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
ITRC20170222-31	**Universal Care, Inc. dba Brand New Day**	CA	2/10/2017	Electronic	Medical/Healthcare	Yes - Published #	**14,005**

On December 28, 2016, Brand New Day became aware that an unauthorized individual had gained access to ePHI provided to one of its HIPAA business associates. Access to ePHI was gained via a third-party vendor system used by Brand New Day's contracting provider six days previously on December 22, 2016. The types of data accessed include plan members' names, addresses, phone numbers, dates of birth and Medicare ID numbers.

Attribution 1 Publication: hhs.gov / CA AG's office / hipaajournal.c Author:
Article Title: Universal Care, Inc. dba Brand New Day
Article URL: http://www.hipaajournal.com/configuration-error-vendor-results-exposure-14000-individuals-ephi-8715/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-30	St. Joseph's Hospital and Medical Center	AZ	2/13/2017	Electronic	Medical/Healthcare	Yes - Published #	623

The electronic protected health information of 623 patients of Dignity Health's St. Joseph Hospital and Medical Center in Phoenix, AZ., has been improperly accessed by one of the center's employees.

Attribution 1 Publication: hhs.gov / hipaajournal.com Author:
Article Title: St. Joseph's Hospital and Medical Center Breach: Improper Access by Employee
Article URL: http://www.hipaajournal.com/theft-hacking-ransomware-improper-access-8706/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-29	Jeffrey D. Rice / Vision Care	OH	2/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	1,586

The files taken from the Vision Care unit contained names, Social Security numbers and limited health information. While a substitute breach notice has been uploaded to the Vision Care website, no mention has been made about the number of individuals impacted.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: Vision Care / Dr. Rice
Article URL: http://www.hipaajournal.com/three-breaches-of-physical-medical-records-impact-4100-individuals-8698/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-28	Equifax	GA	2/8/2017	Electronic	Business	Yes - Published #	158

Equifax provides LifeLock members with credit information through the LifeLock online portal. On January 6, 201 7, LifeLock informed Equifax that it received a report that a LifeLock member was able to view another person's credit report. Equifax has since determined that credit information for 158 LifeLock members, including you, was inadvertently sent to another LifeLock member's online portal as the result of a technical issue.

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: Equifax
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20170208.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-27	University of North Carolina School of Dentristy	NC	2/17/2017	Electronic	Educational	Yes - Published #	200

According to the school, this inadvertent disclosure happened after one of the school's postgraduate dental residents car was broken into. The school sent a letter informing patients that their personal information was stored on either a laptop and/or an SD card for a digital camera device.

Attribution 1 Publication: databreaches.net / abc11.com / wncn.co Author:
Article Title: University of North Carolina School of Dentristy
Article URL: http://abc11.com/news/unc-patients-dental-records-may-have-been-stolen/1760075/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-26	Capital Prosthetic & Orthotic Center, Inc.	OH	2/18/2017	Paper Data	Medical/Healthcare	Yes - Published #	1,134

Thousands of patient files kept by Capital Prosthetic & Orthotic Center, Inc. were stolen from a storage locker in Zanesville in December. The information stolen, according to a release from Capital Prosthetic, may have included patients' names, addresses, dates of birth, phone numbers, Social Security numbers, medical diagnosis/treatments and insurance information.

Attribution 1 Publication: databreaches.net / zanesvilletimesrecor Author:
Article Title: Thousands of medical records stolen
Article URL: http://www.zanesvilletimesrecorder.com/story/news/local/2017/02/17/thousands-medical-records-stolen/97843520/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-25	Hillsborough County Aging Services	FL	2/18/2017	Paper Data	Government/Military	Yes - Published #	650

Hillsborough County Aging Services has notified about 650 clients about a possible breach of protected health information that occurred in 2011.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Information Breach Reported By Hillsborough County
Article URL: https://www.databreaches.net/information-breach-reported-by-hillsborough-county/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-24	Lexington Medical Center	SC	2/18/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

The breach showed that there has been unauthorized access to the employee information database, called eConnect/Peoplesoft. Medical center officials learned about the breach this week and told employees as quickly as possible. This database contains personally identifiable information on current and former employees including names, Social Security numbers and W-2 forms. Importantly, the database does not contain any patient information.

Attribution 1 Publication: databreaches.net / hipaajournal.com / V Author:
Article Title: Lexington Medical Center notifies employees of breach
Article URL: https://www.databreaches.net/sc-lexington-medical-center-notifies-employees-of-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-23	Harvard Computer Society	MA	2/21/2017	Electronic	Educational	Yes - Unknown #	Unknown

More than 1.4 million emails—some divulging Harvard students' grades, financial aid information, and at least one individual's Social Security number—sent over Harvard Computer Society email lists were open to the public until Monday.

Attribution 1 Publication: databreaches.net / Harvard Crimson Author:
Article Title: Email Lists Revealing Students' Private Information Remained Public for Years
Article URL: https://www.thecrimson.com/article/2017/2/21/hcs-emails-public/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-22	Itmanagement.com	NY	2/22/2017	Electronic	Business	Yes - Unknown #	Unknown

A website configuration issue affecting itmanagement.com, a property owned by New York City digital publisher Ziff Davis, can be exploited to access a company database full of private user contact information, including names, phone numbers, employment details, email and employer addresses.

Attribution 1 Publication: databreaches.net / cyberscoop.com Author:
Article Title: Itmanagement.com
Article URL: https://www.cyberscoop.com/millions-of-ziff-davis-ign-pcmag-user-records-sit-exposed-online/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-21	Saturna Capital Corporation	WA	1/27/2017	Electronic	Business	Yes - Unknown #	Unknown

Saturna Capital Corporation (SCC), on behalf of itself, recently became aware that personally identifiable information of two Washington residents was inadvertently sent to an unauthorized person.

Attribution 1 Publication: WA AG's office Author:
Article Title: Saturna Capital Corporation
Article URL: http://agportal-s3bucket.s3.amazonaws.com/Breach%20Saturna%20Capital%20Corp%202017-01-27.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-20	**Catalina Post-Acute & Rehabilitation of Tuscon**	AZ	2/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	**2,953**

The nursing home and rehabilitation center discovered that documents containing the sensitive information of residents and employees had been left unattended and unprotected in a location accessible by the public. A range of sensitive information was detailed in the documents including names, demographic information, Social Security numbers and medical diagnoses.

Attribution 1 Publication: hipaajournal.com / hhs/gov Author:
Article Title: Catalina Post-Acute & Rehabilitation of Tuscon
Article URL: http://www.hipaajournal.com/three-breaches-of-physical-medical-records-impact-4100-individuals-8698/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-19	**Family Service Rochester**	MN	2/17/2017	Electronic	Business	Yes - Published #	**17,037**

On January 26, 2017, we discovered some of the files on our system had been encrypted by ransomware. The unauthorized access affected only a portion of our computer systems. What Information Was Involved? Your information that was potentially accessed includes name, address, phone number, and date of birth.

Attribution 1 Publication: MT AG's office / databreaches.net / MD Author:
Article Title: Family Service Rochester
Article URL: https://dojmt.gov/wp-content/uploads/Family-Services-Rochester.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-18	**Meridian Health Services**	IN	2/22/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,200**

A company spokeswoman said all W-2 forms at Meridian Health Services in Muncie have been compromised. The problem affects about 1,200 employees. Officials with Meridian Health said the same thing happened to them; an employee mistook a phishing email scam for a “legitimate internal company request from a high level executive.”

Attribution 1 Publication: databreaches.net / fox59.com Author:
Article Title: Meridian Health Services in Muncie latest company to fall victim to data breach
Article URL: http://fox59.com/2017/02/22/meridian-health-services-in-muncie-latest-company-to-fall-victim-to-data-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-17	**Mount Healthy City Schools**	OH	2/21/2017	Electronic	Educational	Yes - Published #	**600**

The federal W-2 forms of as many as 600 current and former Mount Healthy City Schools employees may be in the hands of hackers or scam artists. School district administrators said the district's emails have been hacked or phished as part of a nationwide W-2 email phishing scam.

Attribution 1 Publication: databreaches.net / wlwt.com Author:
Article Title: Hundreds of Mt. Healthy school employee W-2s could be in hacker's hands
Article URL: http://www.wlwt.com/article/hundreds-of-mt-healthy-school-employee-w-2s-could-be-in-hackers-hands/8961530

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-16	**Crotched Mountain Foundation**	NH	2/20/2017	Electronic	Business	Yes - Published #	**1,695**

Crotched Mountain Foundation had an unauthorized release of employee W-2s, which include social security numbers, on Thursday, according to center officials. (Exposure number per NY AG's office)

Attribution 1 Publication: ledgertranscript.com / MD AG's office / Author:
Article Title: Crotched Mountain Foundation employees’ personal information released in scam
Article URL: http://www.ledgertranscript.com/gfCrotchedMountain-ml-022117-8164753

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-15	American Senior Communities	IN	2/21/2017	Electronic	Business	Yes - Published #	17,000

American Senior Communities, a nursing home chain based in central Indiana, has announced that one of its employees responded to a W-2 phishing email and sent the tax information of more than 17,000 employees to tax fraudsters.

Attribution 1 Publication: databreaches.net / hipaajournal.com Author:
Article Title: American Senior Communities latest company to fall victim to W-2 phishing scam
Article URL: http://www.hipaajournal.com/american-senior-communities-says-17000-employees-impacted-w-2-scam-8701/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-14	Barron Area School District	WI	2/15/2017	Electronic	Educational	Yes - Unknown #	Unknown

The accidental release of personal information by a so-called “phishing” email has now compromised five Barron Area School District employees, according to the school district central office and the Internal Revenue Service.

Attribution 1 Publication: databreaches.net / news-shield.com / W Author:
Article Title: 'Phishers' catching school employee tax returns
Article URL: http://www.news-shield.com/news/top_stories/article_83604ae2-f390-11e6-b7d5-3feb4a675ac4.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-13	Trenton R-9 School District	MO	2/22/2017	Electronic	Educational	Yes - Unknown #	Unknown

The Trenton R-9 District was regently a targeted victim of an e-mail attack that led to the release of W-2 information for all district employees. Superintendent Dan Wiebers said the incident occurred on Monday, Jan. 23, with an individual pretending to be the superintendent and requesting “what appeared to be a legitimate district email address” for all 2016 district employee W-2 information.

Attribution 1 Publication: databreaches.net / republican-times.com Author:
Article Title: Trenton R-9 E-Mail Attack
Article URL: https://republican-times.com/2017/01/26/trenton-r-9-computer-hacked/ - .WK4N3-QzWOI

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-12	Black River Falls School District	WI	2/1/2017	Electronic	Educational	Yes - Unknown #	Unknown

On Thursday, Jan. 18 the BRF school district was hit with a phishing scandal, sending all staff W-2s to an unknown source. Phishing is the act of emailing someone with the intention of getting vital information from them including social security numbers, bank accounts and, in this case, W-2s.

Attribution 1 Publication: databreaches.net / lacrossetribune.com / Author:
Article Title: Phisher gets W-2s from BRF, tries at Alma Center
Article URL: http://lacrossetribune.com/jacksoncochronicle/news/local/phisher-gets-w--s-from-brf-tries-at-alma/article_8cf50282-59

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-11	CenturyLink	KS	2/20/2017	Electronic	Business	Yes - Published #	8,161

On February 1, 2017, Corporate Security detected and began an investigation into a potentially compromised email account that was being used to generate SPAM. As part of the investigation, we determined that the compromise could have occurred as early as January 30, 2017 when an employee provided account credentials in response to a phishing attack. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-10	Amplify Education	NY	2/17/2017	Electronic	Business	Yes - Published #	560

On February 3, 2017, Amplify discovered a data security incident that involved the exposure of personal information of current and certain former employees through a phishing scam that occurred on February 2, 2017. • Full name, Home address, Social security number, and Wages and taxes earned and paid for 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / VT AG's office / NH AG' Author:
Article Title: Amplify Education
Article URL: https://dojmt.gov/wp-content/uploads/Amplify.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-09	Virginia Wesleyan College	VA	2/17/2017	Electronic	Educational	Yes - Unknown #	Unknown

The tax forms of employees at Virginia Wesleyan College were sent to a third party in response to a phising email scam, school officials said Friday.

Attribution 1 Publication: wavy.com / NH AG's office Author:
Article Title: Tax forms of Virginia Wesleyan employees sent to third party
Article URL: http://wavy.com/2017/02/17/tax-forms-of-virginia-wesleyan-employees-sent-to-third-party/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-08	Maxor National Pharmacy Services	OH	2/17/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On January 31, 2017, the Maxor Compliance Department was notified of a potential cyber attack. After investigation, we discovered that a phishing email was successful in obtaining certain employee information. We have learned that your 2016 W-2 employee information, including your name, address, Social Security number, salary, SS taxes paid, federal taxes paid, withholding taxes, Medicare taxes, and where applicable state taxes, may have been compromised.

Attribution 1 Publication: VT AG'office / MD AG's office / ME AG's Author:
Article Title: Maxor National Pharmacy Services
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Maxor%20National%20Pharmacy%20Services,%20LLC

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-07	Ashland University	OH	2/17/2017	Electronic	Educational	Yes - Published #	2,734

Ashland University officials discovered on Feb. 8 that files containing the W-2 forms of both current and former employees were stolen in an online security breach on Feb. 3. An unauthorized third party unlawfully obtained electronic files containing employee personal information through a criminal scheme known as phishing. (Exposure number per NY AG's office)

Attribution 1 Publication: ashlandcollegian.com / MD AG's office / Author:
Article Title: University records stolen in online security breach: In an online phishing incident, hackers access employee W2s
Article URL: http://www.ashlandcollegian.com/article_b356fc46-f51b-11e6-9b0d-97852b6f6378.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-06	Astadia, Inc.	FL	2/6/2017	Electronic	Business	Yes - Published #	437

On February 2, 2017, an unauthorized individual, impersonating a Astadia executive, contacted an Astadia employee requesting certain information for Astadia employees. Before it was determined that the request was fraudulent, the Astadia employee provided files that contained limited information about some of its employees, including first and last name, address, Social Security number, and 2016 compensation information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: Astadia, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/astadia-20170206.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-05	**Vecellio Group**	FL	2/13/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On February I, 2017, Vecellio Group, Inc. and its subsidiaries were the target of a phishing email that resulted in the unauthorized acquisition by a third party of employees' W-2 tax forms.

Attribution 1 Publication: NH AG's office Author:
Article Title: Vecellio Group
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/vecellio-20170207.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-04	**Goode Compliance International**	FL	2/15/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On January 26, 2017, we discovered that Form W-2 Wage and Tax Statement information for certain employees may have been accessed without authorization on January 25, 2017.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Goode Compliance International
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/goode-20170215.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-03	**JoFit**	PA	2/22/2017	Electronic	Business	Yes - Published #	**4,473**

In mid-January, JoFit first learned that its website may have been the target of a cybersecurity attack aimed at acquiring customer credit card information. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / NH AG's office / SC AG' Author:
Article Title: JoFit
Article URL: https://oag.ca.gov/system/files/JoFit- Adult Notice Form 1.PDF?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-02	**Intex Recreation Corp.**	CA	2/20/2017	Electronic	Business	Yes - Published #	**58,424**

On November 16, 2016, Intex learned of the potential compromise of certain personal information of our customers. Our forensic investigation indicates that unauthorized and malicious code may have been inserted into the company's website and that the incident occurred between approximately April 24, 2016, and December 14, 2016. The information involved may have included your name, address, telephone number, e-mail address, and credit card information. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / OR AG Author:
Article Title: Intex Recreation Corp.
Article URL: https://oag.ca.gov/system/files/sample%20letter_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170222-01	**Deboer Income Tax**	CA	2/17/2017	Electronic	Business	Yes - Unknown #	**Unknown**

Our data security team, Computer Reality, has investigated the breach and uncovered a series of attacks trying to gain access to our systems. The investigation produced a series of IP addresses that had been attacking our system, but the investigation could not ascertain whether they gained successful access and/or what records were exposed.

Attribution 1 Publication: CA AG's office Author:
Article Title: Deboer Income Tax
Article URL: https://oag.ca.gov/system/files/client%20notice%20letter%20DAVE%20EDIT_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170216-08	**Bureau of Indian Affairs**	MT	2/14/2017	Electronic	Government/Military	Yes - Published #	**20,000**

A Bureau of Indian Affairs spokeswoman says more than 20,000 members of two Montana American Indian tribes were notified of a potential data breach involving their personal information. BIA Spokeswoman Nedra Darling says an external hard drive with details on tribal members was stolen last month from an agency law enforcement vehicle in Big Horn County. The unencrypted device contained names, addresses, birthdates and tribal enrollment information for members of the Crow and Northern Cheyenne Tribes.

Attribution 1 Publication: databreaches.net / Miami Herald Author:
Article Title: The Latest: 20,000+ tribal members warned of data breach
Article URL: http://www.miamiherald.com/news/business/technology/article132757214.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170216-07	**Fulton County Clinic**	GA	2/10/2017	Paper Data	Medical/Healthcare	Yes - Unknown #	**Unknown**

Fulton County officials confirmed Friday that they have narrowed their investigation down to one person who they believe is responsible for putting medical records in a dumpster without destroying them first. The paperwork contained names, addresses, phone numbers, social security numbers, symptoms, medications and notes from conversations with psychiatrists.

Attribution 1 Publication: databreaches.net / cbs46.com / hipaajou Author:
Article Title: Fulton County: We know who mishandled patient medical records
Article URL: http://www.cbs46.com/story/34480139/fulton-county-we-know-who-mishandled-patient-medical-records

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170216-06	**Operating Engineers Local Union No. 3**	CO	2/15/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On or about February 9, 2017, OE3 learned that the security of user data stored on our website, www.oe3.org, bad been breached. The information that was involved includes your name, email address, OE3 webpage user name and password.

Attribution 1 Publication: CA AG's office Author:
Article Title: Operating Engineers Local Union No. 3
Article URL: https://oag.ca.gov/system/files/OE3%20Notice%20of%20Data%20Breach%20Letter%20from%20RB_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170216-05	**Asbury Communities**	MD	2/9/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On February 2, 2017, Asbury emailed W-2 information for Asbury employees to a mistaken address. This was a result of a sophisticated "phishing" scheme aimed toward getting private information from organizations.

Attribution 1 Publication: databreaches.net / NH AG's office / MD Author:
Article Title: Asbury Communities
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/asbury-20170209.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170216-04	**Northwestern College**	IA	2/14/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

Beeson says on Tuesday, February 7th, copies of their employees' W2 forms were sent to an unknown party. Beeson says on Tuesday, February 7th, copies of their employees' W2 forms were sent to an unknown party.

Attribution 1 Publication: databreaches.net / kiwaradio.com Author:
Article Title: Northwestern College Employees Are Victims of Phishing
Article URL: http://kiwaradio.com/local-news/northwestern-college-employees-are-victims-of-phishing/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170216-03	Evanson Asset Management	CA	2/14/2017	Electronic	Business	Yes - Published #	222

On January 9th and January 10th, two of our employees' computers were compromised by a phishing email sent to the individuals via a highly-targeted email attack. You are receiving this notice because an email on the impacted computer contained your name email address, and financial account number. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / SC AG's office / MD AG Author:
Article Title: Evanson Asset Management
Article URL: https://dojmt.gov/wp-content/uploads/Evanson-Asset-Management.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170216-02	Honest Kitchen	CA	2/15/2017	Electronic	Business	Yes - Published #	6,750

We recently discovered that The Honest Kitchen experienced an unauthorized network intrusion. As a result of this intrusion, some customers' information was exposed. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / VT AG's office / CA AG' Author:
Article Title: Honest Kitchen
Article URL: https://dojmt.gov/wp-content/uploads/The-Honest-Kitchen.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170216-01	Driveline Retail Merchandising, Inc.	TX	2/14/2017	Electronic	Business	Yes - Published #	15,878

We are writing to inform you of an incident that has likely involved your personal information. On January 25, 2017, an unknown third party sent to Driveline what is commonly called a "phishing" scam. More specifically, an employee received an email that appeared to be sent from Driveline management. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / VT AG's office / MD AG' Author:
Article Title: Driveline Retail
Article URL: https://dojmt.gov/wp-content/uploads/Driveline.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170214-09	Citizens Memorial Hospital	MO	2/14/2017	Electronic	Medical/Healthcare	Yes - Published #	2,504

Personal and financial information was stolen from Citizens Memorial Hospital. Officials say W2 tax forms were mistakenly given to a scammer, and now all employees are at risk. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / hipaajournal.com / NY Author:
Article Title: Citizens Memorial Hospital investigates breach of employee data
Article URL: https://dojmt.gov/wp-content/uploads/Citizens-Memorial.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170214-08	San Antonio Symphony	TX	2/14/2017	Electronic	Business	Yes - Published #	250

Computer hackers broke into the computer network for the San Antonio Symphony this week, stealing the names, birth dates, Social Security numbers, addresses and W-2 tax forms for about 250 employees, the organization confirmed Tuesday.

Attribution 1 Publication: expressnews.com / artsjournal.com Author: David Hendricks
Article Title: Data breach hits San Antonio Symphony employees
Article URL: http://www.expressnews.com/business/local/article/Data-breach-hits-San-Antonio-Symphony-employees-10931740.ph

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170214-07	Scholar Chip	NY	1/31/2017	Electronic	Business	Yes - Unknown #	Unknown

On December 6, 2016, ScholarChip discovered that a technical issue with our online portal may have allowed nine (9) borrowers to access a document containing other borrowers' loan information.

Attribution 1 Publication: NH AG's office / VT AG's office Author:
Article Title: Scholar Chip
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/scholar-chip-20170131.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170214-06	MDF Instruments	CA	2/3/2017	Electronic	Business	Yes - Unknown #	Unknown

On December 7, 2016, MDF was alerted to fraudulent charges occurring on customers' accounts after purchasing MDF products through MDF's website, www.mdfinstruments.com. MDF's IT department investigated the issue and found a malware script on our website that was acquiring credit card data as it was typed.

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: MDF Instruments
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/mdf-instruments-20170203.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170214-05	Massachusetts General Hospital	MA	1/25/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On December 19,2016, MGH learned that an e-mail containing a limited number of patient names and social security numbers was sent to the wrong party in error.

Attribution 1 Publication: NH AG's office / MA AG's office / ME AG Author:
Article Title: Massachusetts General Hospital
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/massachusetts-general-hospital-20170125.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170214-04	Babson College	MA	1/31/2017	Electronic	Educational	Yes - Unknown #	Unknown

I am writing to let you know about a security incident that potentially exposed the personal information of 1 resident of New Hampshire. Our investigation has determined that on January 6, 2017, the College was the subject of a phishing attack in an attempt to divert employee pay. Our security measures ensured that no transfers were made. It was determined, however, that electronic financial account information was potentially accessible to the persons responsible for the breach.

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Babson College
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/babson-20170131.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170214-03	Tufts Health Public Plans, Inc. (formerly Network Health,	MA	1/31/2017	Electronic	Business	Yes - Published #	385

On December 2, 2016, Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) learned from Summit that Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) member data was on a server that had been infected with ransomware. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / MA OCABR / NY AG's Author:
Article Title: Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) / Summit Reinsurance Services
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/tufts-20170131.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170214-02	Frosch International Travel, Inc.	NY	2/13/2017	Electronic	Business	Yes - Published #	841

n February I 0, 2017, a Frosch employee inadvettently provided W-2 information about Frosch employees to an unauthorized third party who was posing as a Frosch employee. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / MD AG's office / NY AG Author:
Article Title: Frosch International Travel, Inc.
Article URL: https://dojmt.gov/wp-content/uploads/Frosch-International-Travel.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170214-01	**Klondex Gold & Silver Mining Co.**	NV	2/6/2017	Electronic	Business	Yes - Unknown #	**Unknown**

We discovered that we were the victim of a data security incident that took place on January 20, 2017, during which an outside actor fraudulently obtained employee W-2 forms. The information on W-2 forms can be used to file a fraudulent tax return, apply for credit cards and loans, among other activities.

Attribution 1 Publication: MT AG's office Author:
Article Title: Klondex Gold & Silver Mining Co.
Article URL: https://dojmt.gov/wp-content/uploads/Klondex-Mines.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170213-08	**Department of Technology, Management and Budget /**	MI	2/3/2017	Electronic	Government/Military	Yes - Unknown #	**Unknown**

A software update implemented in October 2016 that was provided and performed by the vendor supporting the unemployment benefits computer system introduced a vulnerability that allowed authorized users of the Michigan Data Automated System (MiDAS) to access Social Security numbers and names they were not authorized to view.

Attribution 1 Publication: michigan.gov/dtmb Author:
Article Title: Department of Technology, Management and Budget / Michigan Data Automated System (MiDAS)
Article URL: http://www.michigan.gov/dtmb/0,5552,7-150--403986--,00.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170213-07	**Bloomington Public Schools**	MN	2/11/2017	Electronic	Educational	Yes - Published #	**2,800**

Bloomington Public Schools reports employees' personal and financial information has been compromised in a data breach of W-2 tax forms. The information includes names, social security numbers, addresses and earnings.

Attribution 1 Publication: databreaches.net / mprnews.org / startri Author:
Article Title: Data breach of W-2 forms hits thousands of Bloomington school employees
Article URL: http://www.mprnews.org/story/2017/02/11/data-breach-of-w2-forms-hits-thousands-of-bloomington-school-employees

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170213-06	**Patrick Industries**	IN	2/8/2017	Electronic	Business	Yes - Published #	**7,960**

According to Northern Indiana's Better Business Bureau, the W2 phishing scam has cybercriminals disguising emails, making them look like they're from an organization executive. (Exposure number per NY AG's office)

Attribution 1 Publication: databreaches.net / abc57.com / NY AG' Author:
Article Title: W-2 scam at Patrick Industries
Article URL: http://www.abc57.com/story/34460584/w-2-scam-at-patrick-industries

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170213-05	**Mercer County Schools**	WV	2/11/2017	Electronic	Educational	Yes - Unknown #	**Unknown**

"There was a security breach," Paul Hodges, president of the Mercer County Board of Education said Friday evening. The breach occurred when unauthorized individuals asked the employees via internet for their W-2 forms information. Hodges did not know how many employees had been impacted by the scam.

Attribution 1 Publication: databreaches.net / bdtonline.com Author:
Article Title: FBI investigating Mercer County Schools data breach
Article URL: http://www.bdtonline.com/news/fbi-investigating-mercer-county-schools-data-breach/article_2d1805de-f008-11e6-80b8

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170213-04	Independent Services Network	NH	1/31/2017	Paper Data	Business	Yes - Unknown #	Unknown

On January 25, 2017, ISN mailed W-2s to employees. Shortly after they were mailed, it was brought to ISN's attention that employee names, addresses and SSNs were visible through the transparent windows on the envelopes.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: Independent Services Network
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/independent-services-network-20170131.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170213-03	Sweeney Drywall Finishes Corp.	MA	2/7/2017	Electronic	Business	Yes - Unknown #	Unknown

On January 26, 2017, Sweeney Drywall was subject to a phishing attack. An employee in the payroll department received a spoofed email that purported to be from Dan Sweeney, the president of the company.

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: Sweeney Drywall Finishes Corp.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/sweeney-drywall-20170207.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170213-02	Petro Marine	AK	2/13/2017	Electronic	Business	Yes - Unknown #	Unknown

On January 23, 2017, we discovered that Form W-2 Wage and Tax Statement information for certain employees may have been accessed without authorization on January 19, 2017.

Attribution 1 Publication: MT AG's office Author:
Article Title: Petro Marine
Article URL: https://dojmt.gov/wp-content/uploads/Petro-49.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170213-01	NEO Tech	CA	2/13/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On Friday, January 27, 2017, NEO Tech was the victim of an email “phishing” incident that resulted in the release of employee W-2 wage and tax data to an unauthorized email recipient outside the company. This was an isolated incident that did not involve an intrusion into our computer systems or network.

Attribution 1 Publication: CA AG's office / NH AG's office / MD AG Author:
Article Title: NEO Tech
Article URL: https://oag.ca.gov/system/files/NEO%20Tech%20Amended%20Notice%20of%20Data%20Breach%20-%20California_0.p

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-18	AmTote International	MD	2/6/2017	Electronic	Business	Yes - Published #	350

On Wednesday, February 1, 2017, a file containing 2016 IRS Form W-2 information for all US-based AmTote employees was inadvertently emailed to a third party.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: AmTote International
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/amtote-20170206.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-17	Athletic Clubs of America	AR	1/31/2017	Electronic	Business	Yes - Published #	830

On January 5, 2017, Athletic Clubs received an envelope from its vendor that was damaged and empty. The vendor informed Athletic Clubs that when they shipped the envelope to Athletic Clubs, it contained a flash drive with the requested human resources information. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / NY AG's office Author:
Article Title: Athletic Clubs of America
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/athletic-clubs-20170131.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-16	UPI	DC	2/9/2017	Electronic	Business	Yes - Unknown #	Unknown

A hacker is selling a database supposedly containing 83,000 compromised accounts from UPI.com, the website of the 110-year-old American news agency United Press International. For $100 (about 0.09 in bitcoin), a buyer gets emails, names and passwords in a database being sold on AlphaBay, the largest black market on the dark net.

Attribution 1 Publication: databreaches.net / cyberscoop.com Author:
Article Title: Hacker steals 83,000 accounts from UPI news agency
Article URL: https://www.cyberscoop.com/upi-hacked-alpha-bay-darkweb/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-15	Arby's	GA	2/9/2017	Electronic	Business	Yes - Published #	355,000

Sources at nearly a half-dozen banks and credit unions independently reached out over the past 48 hours to inquire if I'd heard anything about a data breach at Arby's fast-food restaurants. Asked about the rumors, Arby's told KrebsOnSecurity that it recently remediated a breach involving malicious software installed on payment card systems at hundreds of its restaurant locations nationwide.

Attribution 1 Publication: krebsonsecurity.com / WI AG's office Author:
Article Title: Fast Food Chain Arby's Acknowledges Breach
Article URL: https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/

Attribution 2 Publication: usatoday.com / WI AG's office / SC AG' Author:
Article Title: Arby's probes possible data breach of credit cards
Article URL: http://www.usatoday.com/story/tech/news/2017/02/09/arbys-breach-may-have-hit-355000-credit-cards/97702594/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-14	University of Iowa	IA	1/19/2017	Electronic	Educational	Yes - Published #	250

The University of Iowa is investigating devices left on campus computers that it believes compromised the personal information for 250 students and staff

Attribution 1 Publication: kcrg.com Author:
Article Title: Device on computers used to steal ID of UI students, staff
Article URL: http://www.kcrg.com/content/news/Device-on-computers-used-to-steal-ID-of-UI-Students-Staff-411228555.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-13	California Correctional Health Care Services (CCHCS)	CA	1/30/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

On January 26, 2017, California Correctional Health Care Services (CCHCS) was informed that on January 23, 2017, a CCHCS staff member inadvertently sent an email containing your personal information to a staff member at another California State department.

Attribution 1 Publication: CA AG's office Author:
Article Title: California Correctional Health Care Services (CCHCS)
Article URL: https://oag.ca.gov/system/files/Breach%20notice_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-12	Platt College	CA	1/17/2017	Paper Data	Educational	Yes - Unknown #	Unknown

A technical error caused Student's 1098T Tuition Statements to be addressed with another student's mailing address, and the Statements were inadvertently mailed to another student on January 13, 2017. 1098T Tuition Statements contain your first and last name, last four digits of your social security number, total amount billed for qualified tuition and related expenses for 2016 and any scholarships or grant totals for 2016.

Attribution 1 Publication: CA AG's office Author:
Article Title: Platt College
Article URL: https://oag.ca.gov/system/files/Platt%20NOB_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-11	Land Title Guarantee Company	CO	2/8/2017	Electronic	Business	Yes - Unknown #	Unknown

In March and May 2016, a Land Title employee received separate e-mails which appeared to come from Land Title's President. These "phishing" e-mails instructed the employee to send W-2 information for Land Title's workforce in 2015. The employee responded mistakenly to two of these e-mails by sending personal information, including your name, Social Security number, and home address.

Attribution 1 Publication: MT AG's office / NH AG's office Author:
Article Title: Land Title Guarantee Company
Article URL: https://dojmt.gov/wp-content/uploads/Land-Title.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-10	Boeing	WA	2/8/2017	Electronic	Business	Yes - Published #	36,000

Boeing recently discovered that a company employee sent an email containing personal information of other employees to his non-Boeing spouse on Nov. 21 , 2016. During Boeing's investigation, the employee stated that he sent a spreadsheet with the personal information to his spouse for help with a formatting issue.

Attribution 1 Publication: threatpost.com / MD AG's office Author:
Article Title: Boeing Notifies 36,000 Employees following breach
Article URL: https://threatpost.com/boeing-notifies-36000-employees-following-breach/123942/

Attribution 2 Publication: MD AG's office Author:
Article Title: Boeing
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280163%20(2).pdf

Attribution 3 Publication: MT AG's office / NH AG's office Author:
Article Title: Boeing
Article URL: https://dojmt.gov/wp-content/uploads/Boeing.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-09	Southeast Alaska Regional Health Consortium	AK	2/8/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

On Wednesday, January 25, 2017, we learned that a targeted "spear phishing" email message had been sent to a SouthEast Alaska Regional Health Consortium employee.

Attribution 1 Publication: MT AG's office / MD AG's office Author:
Article Title: Southeast Alaska Regional Health Consortium
Article URL: https://dojmt.gov/wp-content/uploads/SouthEast-Alaska-Regional-Health-Consortium.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-08	Showpay, LLC	GA	2/8/2017	Electronic	Business	Yes - Published #	1,230

We are writing to inform you that on January 30, 2016, Showpay, LLC was the victim of an email phishing scheme, which resulted in an unauthorized party obtaining a copy of your 2016 W-2 form. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-07	City of Twinsburg, Ohio	OH	2/9/2017	Electronic	Government/Military	Yes - Published #	500

Hundreds of employees of the city of Twinsburg had their W2's stolen in a phishing scam. Officials found out about the scam on Friday morning and immediately contacted the IRS. Around 500 full-time, part-time and seasonal employees were affected.

Attribution 1 Publication: databreaches.net / cleveland19.com Author:
Article Title: More than 500 city of Twinsburg employees have W2's stolen in phishing scam
Article URL: http://www.cleveland19.com/story/34466110/twinsburg-w2-phishing-scam

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-06	Mohave Community College	AZ	2/9/2017	Electronic	Educational	Yes - Unknown #	Unknown

In a letter from MCC President Michael Kearns dated Feb. 3, he warned employees to be on the lookout as a data file containing information about 2016 W-2 forms was inadvertently released as the result of a phishing scam a college employee received in a fraudulent email address listed in Kearns' name.

Attribution 1 Publication: databreaches.net / kdminer.com Author:
Article Title: http://kdminer.com/news/2017/feb/09/mcc-employees-may-be-victims-identity-theft/
Article URL: http://kdminer.com/news/2017/feb/09/mcc-employees-may-be-victims-identity-theft/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-05	Alton Steel, Inc.	IL	2/8/2017	Electronic	Business	Yes - Published #	300

The Alton steel company's data system was victim to a "phishing expedition," according to Alton Steel CEO Jim Hrusovsky, which compromised personal information of its employees. The breach occurred Feb. 2, and Hrusovsky said the company became aware of the breach Monday. The following day, the company began informing the majority of its approximately 300 employees of the breach.

Attribution 1 Publication: databreaches.net / thetelegraph.com Author:
Article Title: Sources: personal info of nearly 300 Alton Steel employees compromised
Article URL: http://thetelegraph.com/news/96467/sources-personal-info-of-nearly-300-alton-steel-employees-compromised

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-04	Corsicana Independent School District	TX	2/8/2017	Electronic	Educational	Yes - Unknown #	Unknown

Late Wednesday Feb. 1, the Corsicana ISD Superintendent Dr. Diane Frost was alerted to an email that was sent from her school email account to another school district employee requesting personal information for employees in the district. The email response included 2016 employee names, social security numbers and earnings. Corsicana ISD quickly learned it was the latest victim of a data seeking scam.

Attribution 1 Publication: databreaches.net / corsicanadailysun.co Author:
Article Title: Corsicana ISD responds to data breach incident
Article URL: http://www.corsicanadailysun.com/news/corsicana-isd-responds-to-data-breach-incident/article_deee240a-ee69-11e6-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-03	Monarch Beverage	IN	2/8/2017	Electronic	Business	Yes - Unknown #	Unknown

In a letter sent to employees, the company explains that a "spear phishing" email was sent to an employee on Jan. 24. The email appeared to be legitimate and from the company's CEO. In the email, the scammer requested copies of employees' W-2 forms for 2016.

Attribution 1 Publication: databreaches.net / cbs4indy.com / MD A Author:
Article Title: Scammer obtains W-2 forms of Monarch Beverage employees
Article URL: http://cbs4indy.com/2017/02/08/scammer-obtains-w-2-forms-of-monarch-beverage-employees/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-02	Verc Enterprises, Inc.	MA	1/27/2017	Electronic	Business	Yes - Unknown #	Unknown

On or about January 21 , 2017, a hacker was able to spoof the email address of member of Verc's management team. The hacker, using the spoofed email address, emailed one of Verc's employees and requested W-2 information and the names, addresses, dates of birth and telephone numbers of all Verc employees.

Attribution 1 Publication: NH AG's office Author:
Article Title: Verc Enterprises, Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/verc-20170127.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170210-01	Adventist Health Tehachapi Valley	CA	2/8/2017	Electronic	Medical/Healthcare	Yes - Published #	250

Adventist Health Tehachapi Valley is investigating a “phishing” scam that could impact about 250 employees. “A 'phishing' scam has led to the release of private Tehachapi Valley Healthcare District information,” said Teresa Adamo, marketing director for AHTV.

Attribution 1 Publication: databreaches.net Author: JILL BARNES NELS
Article Title: Phishing scam targets Adventist Health Tehachapi Valley, could impact hundreds
Article URL: http://www.tehachapinews.com/news/phishing-scam-targets-adventist-health-tehachapi-valley-could-impact-hundreds

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170208-10	West Michigan Whitecaps	MI	2/7/2017	Electronic	Business	Yes - Published #	230

The West Michigan Whitecaps organization is the latest victim of a phishing scam that exposed its employees private information.

Attribution 1 Publication: databreaches.net / wzzm13.com Author:
Article Title: Whitecaps employees victims of W-2 tax scam
Article URL: http://www.wzzm13.com/money/consumer/whitecaps-employees-victims-of-w-2-tax-scam/402810666

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170208-09	College of Southern Idaho	ID	2/7/2017	Electronic	Educational	Yes - Published #	2,509

he College of Southern Idaho has reported a significant phishing scam after an employee inadvertently released W-2 tax information. An individual — who was impersonating a college employee — sent an email Thursday to a CSI employee requesting W-2 forms. (Exposure number per NY AG's office)

Attribution 1 Publication: magicvalley.com / MT AG's office / NY A Author:
Article Title: CSI hit with cyber scam
Article URL: http://magicvalley.com/news/local/education/csi-hit-with-cyber-scam/article_6a0e89b1-54e0-5d4d-b840-f546bc8cf6c3.h

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170208-08	Conover Capital Management, LLC / Conover	WA	2/3/2017	Electronic	Business	Yes - Published #	1,351

On November 16, 2016, an unknown individual purporting to be a Microsoft service technician was granted remote access to a Conover employee's computer. The employee's computer was linked to a client database that contained certain of your personal information, including your name, address, Social Security number and in some instances, drivers' license number. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / WA AG's office / NY A Author:
Article Title: Conover Capital Management, LLC / Conover Securities Corporation
Article URL: https://dojmt.gov/wp-content/uploads/Conover.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170208-07	**Sky Climber, LLC**	DE	2/6/2017	Electronic	Business	Yes - Published #	**1,536**

Today we fell victim to a “phishing” scheme. All employee W2 information which shows everyone’s personal earnings, addresses, and social security numbers was released to a person believed to be one of the Owners (but wasn’t). This highly sensitive information about all of us is now in the hands of people who WILL try to profit from YOUR identify and at your expense. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / MD AG's office / NY AG Author:
Article Title: Sky Climber, LLC
Article URL: https://dojmt.gov/wp-content/uploads/Sky-Climber-LLC.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170208-06	**Berkeley College**	NY	2/6/2017	Electronic	Educational	Yes - Published #	**16,653**

On December 31, 2016, it came to the College's attention that certain student, faculty, and associate data were posted on a public website. While there has been no evidence of theft or disclosure of information of a particularly sensitive nature, the information posted included names, student/associate Berkeley College ID numbers, Berkeley College log-in usernames, Berkeley College e-mail addresses, and default temporary passwords for the same accounts. (Exposure number per NY AG's office)

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170208-05	**Roper St. Francis Healthcare**	SC	1/24/2017	Electronic	Medical/Healthcare	Yes - Published #	**576**

Roper St. Francis Healthcare SC Healthcare Provider 576 01/24/2017 Loss Other Portable Electronic Device

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170208-04	**Multnomah County**	OR	1/20/2017	Electronic	Government/Military	Yes - Published #	**170**

On August 24, 2012, a Health Department employee began automatically forwarding all emails received in the employee’s county email account to a personal Google email account not maintained by the county. Some of these emails included protected health information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA) were forwarded.

Attribution 1 Publication: hhs.gov / hipaajournal.com / Author:
Article Title: Multnomah County
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=A756DD44E2BFC043E0B8E5E0781DFBE7

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170208-03	**Princeton Pain Management**	NJ	1/27/2017	Electronic	Medical/Healthcare	Yes - Published #	**4,668**

On November 28, 2016, PPM discovered that a third party gained unauthorized access to certain data on its computer system. We believe that this incident may have affected certain information stored in our systems including names, addresses, telephone numbers, dates of birth, Social Security or Medicare numbers, driver license or government identification numbers, medical and health insurance identifiers, and diagnostic and treatment information.(Exposure number per NY AG's office)

Attribution 1 Publication: PPN notification / NH AG's office / NY A Author:
Article Title: Princeton Pain Management
Article URL: https://www.doj.nh.gov/consumer/security-breaches/documents/princeton-pain-20170127.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170208-02	**Stephenville Medical & Surgical Clinic**	TX	1/23/2017	Electronic	Medical/Healthcare	Yes - Published #	**75,000**

Stephenville Medical & Surgical Clinic TX Healthcare Provider 75000 01/23/2017 Unauthorized Access/Disclosure Desktop Computer

Attribution 1 Publication: hhs.gov Author:
Article Title: Stephenville Medical & Surgical 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
ITRC20170208-01	**WellCare Health Plans, Inc. / Summit Reinsurance Services**	FL	1/27/2017	Electronic	Medical/Healthcare	Yes - Published #	**24,809**

In a statement, WellCare tells Information Security Media Group that it was alerted on Dec. 27, 2016, that Summit Reinsurance Services, WellCare's former reinsurance services provider, experienced a ransomware attack to its file server on Aug. 8, 2016. "Summit indicated that the encrypted information involved may have included names, dates of birth, addresses, member IDs, diagnoses, provider names and locations, and Social Security numbers of current and former WellCare members," the statement says.

Attribution 1 Publication: hhs.gov / govinfosecurity.com / MD AG's Author:
Article Title: WellCare Health Plans, Inc.
Article URL: http://www.govinfosecurity.com/sizing-up-health-data-breaches-reported-in-2017-so-far-a-9673

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170206-09	**Family Medicine East, Chartered**	KS	2/3/2017	Electronic	Medical/Healthcare	Yes - Published #	**6,800**

On December 8, 2016, an unknown person broke an exterior window to gain entrance to the locked offices of Family Medicine East, Chartered. The intruder took a desktop computer and printer. The notes document many of the patient appointments that took place during those years. They included the name of the patient, the patient's date of birth, the date of the appointment and the name or initials of the physician or PA who saw the patient on that date.

Attribution 1 Publication: databreaches.net / hipaajournal.com / h Author:
Article Title: Family Medicine East, Chartered in Wichita notifies patients of stolen computer
Article URL: https://www.databreaches.net/family-medicine-east-chartered-in-wichita-notifies-patients-of-stolen-computer/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170206-08	**Alaska Department of Public Safety**	AK	2/3/2017	Electronic	Government/Military	Yes - Published #	**1,020**

More than 1,000 people were identified as potentially having personal information "compromised" after an employee with the Division of Statewide Services removed several documents from the office, according to Alaska State Troopers.

Attribution 1 Publication: databreaches.net Author:
Article Title: Ex-employee of Alaska Department of Public Safety employee stole personal information during robbery – AST
Article URL: https://www.databreaches.net/ex-employee-of-alaska-department-of-public-safety-employee-stole-personal-informatio

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170206-07	**Anchor Packaging**	AR	2/2/2017	Electronic	Business	Yes - Unknown #	**Unknown**

A company in Paragould reported Thursday that someone was attempting to impersonate the company's president in an apparent email phishing scam.

Attribution 1 Publication: wmcactionnews5.com Author:
Article Title: Anchor Packaging reports email phishing scam
Article URL: http://www.wmcactionnews5.com/story/34415018/anchor-packaging-reports-email-phishing-scam

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170206-06	Manatee County School District	FL	2/4/2017	Electronic	Educational	Yes - Published #	7,700

Manatee County School District employees' W-2 tax forms may have been compromised as a result of a cyberattack, the district announced to its employees Friday evening.

Attribution 1 Publication: databreaches.net / bradenton.com Author:
Article Title: Cyberattack on Manatee County School District may compromise employee tax forms
Article URL: http://www.bradenton.com/news/local/article130785724.html

Attribution 2 Publication: washingtontimes.com / VT AG's office / Author:
Article Title: anatee County schools faces data breach affecting thousands
Article URL: http://www.washingtontimes.com/news/2017/feb/12/manatee-county-schools-faces-data-breach-affecting/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170206-05	On Gossamer	FL	1/26/2017	Electronic	Business	Yes - Unknown #	Unknown

On or around December 1, 2016, we received reports of suspicious activity from our third party e-commerce partner. The information collected included the cardholder's name, shipping address, billing address, email address, card number, card type, expiration date, and CVV. If you were a registered user at our site, your login and password would also have been collected.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170206-04	Le Mystere	OK	1/26/2017	Electronic	Business	Yes - Unknown #	Unknown

On or around December 1, 2016, we received reports of suspicious activity from our third party e-commerce partner. The information collected included the cardholder's name, shipping address, billing address, email address, card number, card type, expiration date, and CVV. If you were a registered user at our site, your login and password would also have been collected.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170206-03	M. Stanley Metz & Company, Inc.	MA	2/1/2017	Electronic	Business	Yes - Unknown #	Unknown

On December 14, 2016, M. Stanley Metz & Co. discovered that the program hosting client tax returns may have been subject to unauthorized access within our network. The information contained within your tax return includes your name, address and Social Security number.

Attribution 1 Publication: VT AG's office / NH AG's office / MA OC Author:
Article Title: M. Stanley Metz & Company, Inc.
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/M%20Stanley%20Metz%20and%20Company%20SBN%

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170206-02	Carole Hochman	OK	1/26/2017	Electronic	Business	Yes - Unknown #	Unknown

On or around December 1, 2016, we received reports of suspicious activity from our third party e-commerce partner. The information collected included the cardholder's name, shipping address, billing address, email address, card number, card type, expiration date, and CVV.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170206-01	**Nakawatase & Kaminsky, CPAs, LLP**	CA	2/3/2017	Electronic	Business	Yes - Unknown #	**Unknown**

In January 2017, we confirmed through the use of our forensic information technology investigation firm, Navigant, that the Lacerte tax system we utilize for maintaining and filing tax returns was compromised by an intruder on October 31, 2016, November 1, 2016, November 5, 2016, and November 8, 2016.

Attribution 1 Publication: CA AG's office Author:
Article Title: Nakawatase & Kaminsky, CPAs, LLP
Article URL: https://oag.ca.gov/system/files/ACL1000_L_PCIDFSSTAGE_109_20170131_001_archive_v2_IDX_001_PDF_001_800201

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170203-11	**PIP Printing and MarketingServices**	CA	2/3/2017	Electronic	Business	Yes - Unknown #	**Unknown**

MacKeeper Security Research Center reports that PIP Printing and Marketing Services, a franchise of Franchise Services in California, was leaking data. These contain around 50+GB of scanned documents relating to court cases, medical records, well known companies, and celebrities. There is an archive of correspondence where company's clients ask managers to make copies of the attached documents. This archive contains more than 2,200 messages and some of them have credit card numbers and billing details in plain text. And more…

Attribution 1 Publication: databreaches.net Author:
Article Title: PIP Printing and Marketing Services exposed 400GB of data, including personal information
Article URL: https://www.databreaches.net/pip-printing-and-marketing-services-exposed-400gb-of-data-including-personal-informa

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170203-10	**SSM Dean Medical Group**	WI	1/10/2017	Electronic	Medical/Healthcare	Yes - Published #	**4,800**

SSM Dean Medical Group WI Healthcare Provider 4800 01/10/2017 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: SSM Dean Medical 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
ITRC20170203-09	**Verity Medical Foundation / Verity Health System**	CA	1/11/2017	Electronic	Medical/Healthcare	Yes - Published #	**10,164**

Although there is no evidence that patient information was used in an unauthorized fashion, Verity Health System is notifying more than 9,000 individuals that their personal information may have been accessed by an unauthorized third party. The information, dated between 2010 and 2014, includes patient names, dates of birth, medical record numbers, addresses, email addresses, phone numbers and the last four digits of credit card numbers.

Attribution 1 Publication: hhs.gov/ databreaches.net/ HS press rel Author:
Article Title: Verity Health System Notifies Thousands of Patients of Web Site Hack That Began in 2015
Article URL: https://www.databreaches.net/verity-health-system-notifies-thousands-of-patients-of-web-site-hack-that-began-in-2015

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170203-08	**St. Luke's Hospital**	ND	1/16/2017	Electronic	Medical/Healthcare	Yes - Published #	**600**

St. Luke's Hospital ND Healthcare Provider 600 01/16/2017 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: St. Luke's 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
ITRC20170203-06	Vertiv Co. Health & Welfare Plan	OH	1/31/2017	Paper Data	Medical/Healthcare	Yes - Published #	955

Vertiv Co. Health & Welfare Plan OH Health Plan 955 01/31/2017 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Vertiv Co. Health & Welfare 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
ITRC20170203-05	Office of Shiel Sexton	IN	1/27/2017	Electronic	Medical/Healthcare	Yes - Published #	710

Shiel Sexton IN Health Plan 710 01/27/2017 Unauthorized Access/Disclosure Other

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170203-04	R.O.A.D.S. Foundation dba ROADS Community Care	CA	1/26/2017	Paper Data	Medical/Healthcare	Yes - Published #	670

THE R.O.A.D.S. Foundation Inc. DBA R.O.A.D.S. Community Care Clinic CA Healthcare Provider 670 01/26/2017 Loss Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: R.O.A.D.S. Foundation
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170203-03	Distribution International	TX	1/27/2017	Electronic	Business	Yes - Published #	1,133

On or about January 25, 2017, a data breach occurred, which allowed a hacker to obtain year-end tax reporting information via afictitious or “spoofed” e-mail. The information likely included your name, postal address, social security number, marital status, employer information, annual compensation, employee benefit information, and certain tax return data, such as withholding information, exemptions, and allowances. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / MD AG's office / NY AG Author:
Article Title: Distribution International
Article URL: https://dojmt.gov/wp-content/uploads/Distribution-International.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170203-02	Axis Insurance Services	NJ	1/30/2017	Electronic	Business	Yes - Unknown #	Unknown

On December 12, 2016, several Axis employees received a spam phishing email to their Axis email accounts. One Axis employee clicked on the link in the phishing email and entered her email credentials. The affected email account contained a copy of a business check, which contained your name, bank account number, and bank routing number.

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170203-01	King, McNamara, Moriarty LLP	MA	2/2/2017	Electronic	Business	Yes - Published #	6,791

We were victims of a malicious hacking incident several months ago. The following information appears to have been accessed: tax return information which included names, addresses, dates of birth, and Social Security numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / MA OCABR / MD AG's Author:
Article Title: King, McNamara, Moriarty LLP
Article URL: https://dojmt.gov/wp-content/uploads/King-McNamara-Moriarty.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-11	Harlingen Texas Motors	TX	2/2/2017	Paper Data	Business	Yes - Unknown #	Unknown

Dozens of documents containing people's personal information were found sitting in a dumpster in Harlingen. "They told me I had a new credit card and the chip changed on it so they didn't run it. So they sold it out or foreclosed on it or whatever they call it. So somebody purchased it on Saturday and they threw my files away," Andre Cano, the owner of Harlingen Texas Motors, said.

Attribution 1 Publication: databreaches.net / KRGV.com Author:
Article Title: Man Finds Documents with Personal Information Inside Dumpster
Article URL: http://www.krgv.com/story/34404626/man-finds-documents-with-personal-information-inside-dumpster

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-10	Renovate America	CA	1/23/2017	Electronic	Business	Yes - Published #	800

Renovate America alerted nearly 800 current and former employees that it had wrongly provided W-2 forms to someone posing as the CEO, John Paul McNeill, following what looked like a legitimate email request.
"Unfortunately, copies of all 2016 W-2 forms were provided before we discovered that the request was made from a fraudulent account by someone using an email address that appeared to belong to our CEO," the notification said.

Attribution 1 Publication: sandiegouniontribune.com / MD AG's off Author:
Article Title: Solar finance firm sent all employees' W-2s to
Article URL: http://www.sandiegouniontribune.com/news/watchdog/sd-me-w2-breach-20170123-story.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-09	Belton Independent School District	TX	2/2/2017	Electronic	Educational	Yes - Published #	1,700

Employees of a Central Texas school district were fooled by an email scam into releasing personal information for approximately 1,700 current and former district workers.

Attribution 1 Publication: databreaches.net / nbcdfw.com Author:
Article Title: Texas School District Duped into Releasing Personal Data
Article URL: http://www.nbcdfw.com/news/local/Texas-School-District-Duped-into-Releasing-Personal-Data-412559853.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-08	Davidson County School System	NC	2/1/2017	Electronic	Educational	Yes - Published #	3,262

"We recently discovered that our company was the victim of an email spoofing attack on January 31, 2017, by an individual pretending to be our Superintendent. A request was made for all 2016 Davidson County Board of Education employee W-2 information. Unfortunately, copies of all 2016 employee W2 forms were provided before we discovered that the request was made from a fraudulent account by someone using the name of our Superintendent." (Exposure number per NY AG's office)

Attribution 1 Publication: the-dispatch.com Author:
Article Title: Don't take the bait: Data breach raises questions about cybersecurity
Article URL: http://www.the-dispatch.com/news/20170211/dont-take-bait-data-breach-raises-questions-about-cybersecurity

Attribution 2 Publication: myfox8.com / the-dispatch.com / NY AG' Author:
Article Title: Davidson Co. Sheriff's Office investigating 'email spoofing attack' involving school system employees' W-2s
Article URL: http://myfox8.com/2017/02/01/davidson-county-sheriffs-office-investigating-email-spoofing-attack-involving-school-sy

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-07	TransPerfect Global Inc.	NY	1/27/2017	Electronic	Business	Yes - Published #	4,884

An individual or group of individuals pretending to be co-CEO Elizabeth Elting sent an e-mail requesting W-2 tax form information for workers who were employed at the company in 2015, according to internal communication obtained by The News Journal. (Exposure number per NY AG's office)

Attribution 1 Publication: delawareonline.com/MT AG's office/NH Author:
Article Title: TransPerfect workers victimized in data breach
Article URL: http://www.delawareonline.com/story/money/2017/01/27/transperfect-workers-victimized-data-breach/97129850/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-06	Persante	NJ	1/31/2017	Electronic	Medical/Healthcare	Yes - Published #	350

We are contacting you to let you know that Persante Health Care ("Persante") has been the targeted victim to an email spoofing incident. This scam resulted in the breaching of your personal information contained on your W2 Form, which includes your name, home address and social security number. (Exposure number per NY AG's office)

Attribution 1 Publication: MT AG's office / MD AG's office / NY AG Author:
Article Title: Persante
Article URL: https://dojmt.gov/wp-content/uploads/Persante.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-05	Mitchell Gold + Bob Williams	NC	1/31/2017	Electronic	Business	Yes - Published #	1,109

An email spoofing attack led to the theft of personal information of employees at Taylorsville furniture company Mitchell Gold + Bob Williams, officials said Tuesday. (Exposure number per NY AG's office)

Attribution 1 Publication: statesville.com / scmagazine.com / NY Author:
Article Title: Employee information stolen from Taylorsville furniture company
Article URL: http://www.statesville.com/news/employee-information-stolen-from-taylorsville-furniture-company/article_8760f202-e7

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-04	Pointe Coupee General	LA	1/30/2017	Electronic	Medical/Healthcare	Yes - Published #	235

Pointe Coupee General Hospital is in the process of formally notifying 235 employees of a data security incident that affected their W-2 information.

Attribution 1 Publication: databreaches.net / WBRZ.com / compa Author:
Article Title: Hackers posing as administrator get 200 workers' W-2 forms
Article URL: http://www.wbrz.com/news/hackers-posing-as-administrator-get-200-workers-w-2-forms/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-03	Kuhana Associates	HI	2/2/2017	Electronic	Medical/Healthcare	Yes - Unknown #	Unknown

We are contacting you about a data breach that has occurred in which your personal information may have been compromised. Personal information was inadvertently sent to an individual posing as one of our company officers. The email response contained W-2 information.

Attribution 1 Publication: databreaches.net / MT AG's office / MD Author:
Article Title: Kuhana Associates
Article URL: https://dojmt.gov/wp-content/uploads/Kuhana.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-02	Toys "R" Us	DE	1/17/2017	Electronic	Business	Yes - Unknown #	Unknown

The vendor who manages our Rewards“R”Us loyalty program recently advised us of unauthorized attempts to access Rewards“R”Us loyalty member accounts. Account information may include the loyalty members’ name, email addresses, mailing address and phone number(s). If you have a Geoffrey’s Birthday Club account and it is linked to your Rewards“R”Us account, then information in this account, such as your child’s name and birth date, may have been accessed as well.

Attribution 1 Publication: CA AG's office Author:
Article Title: Toys "R" Us
Article URL: https://oag.ca.gov/system/files/Notice%20of%20Unauthorized%20RewardsRUs%20Access%20%28Final%20Versions%

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170202-01	DBM Global	AZ	1/24/2017	Electronic	Business	Yes - Published #	5,895

On January 7, 2017, our Phoenix office was burglarized and one employee laptop was stolen. The stolen laptop data may have included personal information such as employee, former employees, and their respective dependents from December 2014 to present. Specifically, the information may have included: name, address, social security number, employee identification number, date of birth, and direct deposit bank information. The stolen data may also have included name, address, social security number and date of birth for dependents of the employees and former employees. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / OR AG's office / SC AG Author:
Article Title: DBM Global
Article URL: https://www.oag.ca.gov/system/files/DBM%20Global%20Data%20Breach%20Notice%20Letter_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170201-03	Morton Community Unit School District 709	WA	1/31/2017	Electronic	Educational	Yes - Unknown #	Unknown

A security breach involving an email in the Morton School District occurred Tuesday morning. An email appearing to come from Superintendent Lindsey Hall to an employee asking for W-2 information actually came from an outside entity. An investigation by the Morton Police Department has revealed the source of the fraudulent email appears to have come from Russia. Names and social security numbers were released when the employee complied with the email request.

Attribution 1 Publication: washingtontimesreporter.com Author:
Article Title: Morton Community Unit School District 709 reports security breach
Article URL: http://www.washingtontimesreporter.com/news/20170131/morton-community-unit-school-district-709-reports-security-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170201-02	XBOX 360 / PlayStation ISO Forum Accounts	WA	1/31/2017	Electronic	Business	Yes - Unknown #	Unknown

An unidentified hacker reportedly breached the XBOX 360 and PlayStation Portable ISO forums compromising 2.5 million gamer accounts. The breaches occurred approximately around September 2015 and compromised email addresses, account passwords and IP addresses, according to independent researcher Troy Hunt.

Attribution 1 Publication: SCmagazine.com Author:
Article Title: 2.5 million XBOX 360 and PSP ISO forum accounts breached
Article URL: https://www.scmagazine.com/xbox-and-psp-forum-accounts-breached/article/635024/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170201-01	Palomar Community College	CA	1/5/2017	Electronic	Educational	Yes - Published #	3,053

On January 19, 2017, we learned that an unauthorized individual may have accessed part of our network that contained IRS Form W-2s for some of our employees. Upon learning of this, we immediately began an investigation and contacted law enforcement. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / sandiegouniontribune.c Author:
Article Title: Palomar Community College
Article URL: https://oag.ca.gov/system/files/CA%20Notice_1.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170131-01	Scotty's Brewhouse	IN	1/31/2017	Electronic	Business	Yes - Published #	4,000

Officials at Scotty's Brewhouse are working to inform thousands of employees across the company about an email data breach, leaking employees' W-2 forms to an unknown suspect. According to the police report, an individual posing as company CEO Scott Wise sent an email to a payroll account employee. The email requested the employee to send all 4,000 employees W-2 forms in PDF form.

Attribution 1 Publication: fox59.com / scmagazine.com Author:
Article Title: Every Scotty's Brewhouse employee affected by data breach; scammer gets copy of all W-2 forms
Article URL: http://fox59.com/2017/01/31/every-scottys-brewhouse-employee-affected-by-data-breach-scammer-gets-copy-of-all-w-2

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-17	Potomac Healthcare	VA	1/5/2017	Electronic	Medical/Healthcare	Yes - Published #	266

Chris Vickery of MacKeeper discovered 11GB of internal Potomac data were left unprotected and could be accessed over the Internet without a username or a password. The data included names, Social Security numbers, locations, assigned units, and salaries of psychologists, doctors, and other healthcare professionals. The files also included lists of websites and programs with their associated usernames and passwords. (Exposure number per NY AG's office)

Attribution 1 Publication: hipaajournal.com / MD AG's office / NY Author:
Article Title: 11GB of Sensitive Data Left Unprotected by Department of Defense Subcontractor
Article URL: http://www.hipaajournal.com/11gb-data-left-unprotected-department-defense-subcontractor/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-16	Emory Healthcare	GA	1/9/2017	Electronic	Medical/Healthcare	Yes - Published #	79,930

A hacker by the name of Harak1r1 has taken advantage of a misconfigured MongoDB healthcare database containing 200,000 records of Emory Healthcare patients. The database contained the protected health information of patients of the Emory Brain Health Center. Information in the database includes patients' names, addresses, email addresses, dates of birth, medical ID numbers, and phone numbers. (number of records per hhs.gov)

Attribution 1 Publication: hipaajournal.com / MT AG's office / hhs. Author:
Article Title: Emory Healthcare Joins 28,000 Other Victims of MongoDB Ransom Attacks
Article URL: http://www.hipaajournal.com/emory-healthcare-joins-28000-victims-mongodb-ransom-attacks-8639/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-15	TriHealth of Cincinnati	OH	1/26/2017	Paper Data	Medical/Healthcare	Yes - Published #	1,126

A 'software glitch' has resulted in billing statements and other communications sent by TriHealth of Cincinnati being mailed to patients' former addresses. The privacy breach was discovered in November 2016, and impacts 1,126 TriHealth patients. The types of protected health information contained in the mailings varied from patient to patient. PHI that was potentially exposed was limited to patients' names, visit dates, descriptions of medical service provided, places of service, financial charges, details of payments and adjustments, account balances, due payments, and details of appointments.

Attribution 1 Publication: hipaajournal.com Author:
Article Title: Mailing Error Sees 1,126 Letters Sent to Patients' Previous Addresses
Article URL: http://www.hipaajournal.com/mailing-error-sees-1126-letters-sent-to-patients-previous-addresses-8665/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-14	Covenant HealthCare	MI	1/26/2017	Electronic	Medical/Healthcare	Yes - Published #	6,197

Covenant HealthCare has notified more than 6,000 patients that their electronic medical records were inappropriately accessed by one of its employees. The improper access continued for nine months until November 21, 2016 and involved 6,197 patients. A range of data were potentially viewed including patient's names, dates of birth, home addresses, health insurance information, diagnostic and treatment information, medical record numbers, Social Security numbers and driver's license numbers.

Attribution 1 Publication: hipaajournal.com / hhs.gov Author:
Article Title: Hospital Employee Discovered to Have Improperly Accessed 6,200 Patient Records
Article URL: http://www.hipaajournal.com/hospital-employee-discovered-improperly-accessed-6000-patient-records-8666/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-13	Safari Ltd.	FL	1/4/2017	Electronic	Business	Yes - Unknown #	Unknown

Safari recently learned that an unauthorized individual was able to gain access to portions of its website and may have been able to access certain customer information as a result. The incident could affect certain personal information, including name, address, email address, telephone number, payment card account number, expiration date, and verification code for a limited number of individuals.

Attribution 1 Publication: NH AG's office / MD AG's office / NY AG Author:
Article Title: Safari Ltd.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/safari-20170104.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-12	Stax Inc.	NY	1/9/2017	Electronic	Business	Yes - Unknown #	Unknown

On November 15,2016, an employee in the Stax accounting department was the victim of a phishing email, which enabled unknown criminals to access the employee's email account.

Attribution 1 Publication: NH AG's office Author:
Article Title: Stax Inc.
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/stax-20170109.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-11	Haverford College	PA	1/10/2017	Electronic	Educational	Yes - Unknown #	Unknown

On August 2, 2016, Haverford College discovered that a Google Group email list that was intended to be private was open to the entire Haverford community. Haverford IT immediately secured access to the group to prevent continuing unauthorized access. While Haverford's investigation is ongoing, Haverford has determined that there was a misconfiguration in a Google Group site that allowed unauthorized members of the Haverford community to access to certain files containing personal information related to individuals who have filed IRS form W -9s with the College. Information that may have been accessed included your name, address, and Social Security number.

Attribution 1 Publication: NH AG's office / MD AG's office Author:
Article Title: Haverford College
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/haverford-college-20170110.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-10	Honor Flight New England	NH	1/24/2017	Electronic	Business	Yes - Published #	649

On January 4, 2017, Honor Flight experienced a computer server malfunction and contacted an information technology service provider for assistance. he service provider performed an investigation and identified signs of unauthorized access to Honor Flight's server on November 15, 2016, December 6, 2016, December 11,2016 and January4, 2017. (Exposure number per NY AG's office)

Attribution 1 Publication: NH AG's office / VT AG's office / MD AG' Author:
Article Title: Honor Fligth New England
Article URL: http://www.doj.nh.gov/consumer/security-breaches/documents/honor-flight20170124.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-09	VICI Marketing LLC	FL	1/27/2017	Electronic	Business	Yes - Unknown #	Unknown

Researchers from the MacKeeper Security Research Center have made one of the biggest discoveries to date with several hundred thousand files publically available. The files belong to a controversial Florida based marketing company VICI Marketing LLC and include thousands of audio recordings where customers give their names, addresses, phone number, credit card numbers, CV numbers and more.

Attribution 1 Publication: databreaches.net Author:
Article Title: Telemarketing Company Leaks Nearly 400K Consumer Files
Article URL: https://www.databreaches.net/telemarketing-company-leaks-nearly-400k-consumer-files/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-08	Claremont Rug Co. / Paychex	NY	1/28/2017	Electronic	Business	Yes - Unknown #	Unknown

This year may be extra taxing for Paychex, a corporate payroll service that twice shipped scores of confidential salary records and other documents to the wrong address. The Rochester, N.Y.-based finance and employee-benefits firm delivered more than 60 federal W-2 forms and other tax records issued by a Northern California employer to a San Diego woman whose daughter briefly worked for the company last year.

Attribution 1 Publication: databreaches.net / sandiegouniontribune Author:
Article Title: Payroll service ships W-2 to wrong address by mistake — twice
Article URL: http://www.sandiegouniontribune.com/news/watchdog/sd-me-paychex-error-20170127-story.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-07	General Services Administration	DC	1/27/2017	Electronic	Government/Military	Yes - Unknown #	Unknown

A series of four audits by the General Services Administration's inspector general have found that the agency's cloud computing system made personally identifiable information accessible to employees and contractors not authorized to have it. The audits, which were instituted after the OIG found multiple instances where sensitive information was accessible on GSA's cloud computing system, date back to 2014 and were publicly released on Jan. 27.

Attribution 1 Publication: databreaches.net / federaltimes.com Author:
Article Title: GSA IT gaps leaked personal information, OIG says
Article URL: http://www.federaltimes.com/articles/gsa-cloud-computing-gaps-leaked-personal-information-oig-says

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-06	Mercedes Independent School District	TX	1/27/2017	Electronic	Educational	Yes - Published #	1,000

A Rio Grande Valley school district said sensitive employee information was unintentionally released. Mercedes ISD announced Friday they accidentally released close to 1000 W-2 forms of their employees. Mercedes ISD superintendent Dr. Daniel Trevino Jr. said they received an email requesting W-2s of school district employees. He said staff later realized the email was sent from an unauthorized account.

Attribution 1 Publication: databreaches.net / krgv.com Author:
Article Title: Mercedes School Employees' Information Sent to Unauthorized Source
Article URL: http://www.krgv.com/story/34366270/mercedes-school-employees-information-sent-to-unauthorized-source

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-05	Lexington School District Two	SC	1/30/2017	Electronic	Educational	Yes - Published #	1,300

Lexington School District Two officials have confirmed that there has been an electronic security breach within the district. According to the memo obtained by WACH FOX, the breach involves social security numbers and financial information pertaining to federal income taxes

Attribution 1 Publication: databreaches.net / wach.com / wltx19.co Author:
Article Title: Midlands school district hacked, leaving employees exposed
Article URL: http://wach.com/news/local/midlands-school-district-hacked-leaving-employees-exposed

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-04	Sunrun	CA	1/27/2017	Electronic	Business	Yes - Published #	4,000

A hacker posing as Sunrun CEO Lynn Jurich obtained the W-2 tax forms — including Social Security numbers and salary details — for many employees of the San Francisco solar firm, the company said Friday.

Attribution 1 Publication: databreaches.net/sfgate.com/ krebsonse Author:
Article Title: Hacker impersonates Sunrun CEO, nabs employee W-2 tax forms
Article URL: http://www.sfgate.com/business/article/Sunrun-hack-nabs-employee-W-2-tax-forms-10889441.php

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-03	Campbell County Health	WY	1/26/2017	Electronic	Medical/Healthcare	Yes - Published #	1,457

Social Security numbers and W-2 information for about 1,400 employees who worked over the past year at Campbell County Health were mistakenly released sometime Wednesday to someone impersonating a hospital executive.

Attribution 1 Publication: databreaches.net / gillettenewsrecord.co Author:
Article Title: Hospital scammed for employee information
Article URL: http://www.gillettenewsrecord.com/news/local/article_fa834027-f83a-519b-a65d-d94bc5293af3.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-02	Odessa School District	MO	1/25/2017	Electronic	Educational	Yes - Unknown #	Unknown

The Odessa School District is the latest victim of an e-mail hack. Hackers now have access to employee's social security numbers, wages, and even their W-2's.

Attribution 1 Publication: databreaches.net / kmbc.com Author:
Article Title: Odessa one of eight school districts targeted in e-mail phishing scam
Article URL: http://www.kmbc.com/article/odessa-one-of-eight-school-districts-targeted-in-e-mail-phishing-scam/8640938

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170130-01	eHealthInsurance	CA	1/30/2017	Electronic	Business	Yes - Unknown #	Unknown

The notice says an eHealth employee received a phishing email that the individual thought was "a legitimate email" from a company executive. Before the company discovered that the request was made from a fraudulent email account, the employee had already sent copies of eHealth employees' W-2 tax forms.

Attribution 1 Publication: CA AG's office / healthinfosecurity.com / Author:
Article Title: eHealthInsurance
Article URL: https://oag.ca.gov/system/files/eHealthInsurance%20-Notice%20only%20-%20CA%20-%20Exhibit%201_0_0.pdf?

Attribution 2 Publication: CA AG's office / healthcareitnews.com Author:
Article Title: eHealthInsurance, Campbell County Health each fall for W-2 phishing scams
Article URL: http://www.healthcareitnews.com/news/ehealthinsurance-campbell-county-health-each-fall-w-2-phishing-scams

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170127-08	UGI Utilities	PA	1/26/2017	Electronic	Business	Yes - Published #	1,825

UGI Utilities said Thursday that the personal information of about 1,900 employees and former employees was "acquired" by the perpetrators of an email phishing scheme that targeted the company Tuesday. (Exposure number per NY AG's office)

Attribution 1 Publication: mcall.com / MD AG's office / NY AG's of Author:
Article Title: Employees, not customers, hit in this data breach
Article URL: http://www.mcall.com/business/mc-ugi-employees-exposed-phishing-scam-watchdog-20170126-column.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170127-07	Marin Software, Inc.	CA	1/27/2017	Electronic	Business	Yes - Published #	795

Marin Software, an online ad management platform, suffered a data breach that may have compromised the personal information of many staffers and ex-staffers. The company alerted employees and former employees that their personal data, including W-2, Social Security number, address, email, salary and date of birth, was swiped by someone posing as a company executive. (Exposure number per NY AG's office)

Attribution 1 Publication: adexchanger.com / MD AG's office / NY Author:
Article Title: Marin Software Suffered A Data Breach; Epsilon Had A Disappointing Year
Article URL: https://adexchanger.com/ad-exchange-news/friday-01272017/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170127-06	**MultiCare Health System**	WA	1/26/2017	Electronic	Medical/Healthcare	Yes - Published #	**1,249**

An unauthorized person may have gained access to an employee's email account on Nov. 27, 2016. The account may have contained personal patient information, including name, date of birth, address, gender, date of service, account balance, and diagnosis and treatment information.

Attribution 1 Publication: king5.com / hhs.gov Author:
Article Title: MultiCare breach allows access to personal records for 1,200 patients
Article URL: http://www.king5.com/news/health/multicare-breach-allows-access-to-personal-records-for-1200-patients/393722371

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170127-05	**Wonderful Health and Wellness / Wonderful Center**	CA	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	**3,358**

On December 12, 2016, it was discovered that a laptop containing medical information from the Wonderful Center for Health Innovation was stolen between December 9, 2016 and December 12, 2016. The files on the laptop included your full name, home address, date of birth, telephone number, electronic mail (email) address, clinic account number, medical conditions, medical test results, and clinic treatment date(s).

Attribution 1 Publication: CA AG's office / hipaajournal.com / hhs. Author:
Article Title: Wonderful Health and Wellness / Wonderful Center for Health Innovation
Article URL: https://oag.ca.gov/system/files/TWC%20Redaction_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170127-04	**Pool Supply Unlimited**	CA	1/9/2017	Electronic	Business	Yes - Unknown #	**Unknown**

On January 11, 2017 Pool Supply Unlimited learned that a third party computer server utilized for our website was hacked. In the last week poolsupplyunlimited.com has been held hostage by a group of hackers in Iran. We are providing this notice to inform you that your poolsupplyunlimited.com user name and password were compromised.

Attribution 1 Publication: CA AG's office Author:
Article Title: Pool Supply Unlimited
Article URL: https://oag.ca.gov/system/files/Pool%20Supply%20redacted_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170127-03	**Charles Komar & Sons / Cuddl Duds**	NJ	1/26/2017	Electronic	Business	Yes - Published #	**25,127**

On or around December 1, 2016, we received reports of suspicious activity from our third party e-commerce partner. We immediately began to investigate these reports to identify what happened and what information was impacted. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MD AG's office / NY AG Author:
Article Title: Cuddl Duds / Charles Komar & Sons
Article URL: https://oag.ca.gov/system/files/Komar%20-%20Notice%20only%20-%20CA%20Exhibit%201_0_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170127-02	**Synergy Specialists Medical Group**	CA	1/27/2017	Electronic	Medical/Healthcare	Yes - Published #	**569**

On December 9, 2016, we became aware that some patients had received an email from our office earlier that morning that we did not send. Any information you sent to or received from our office on drjsbdpm@gmail.com. This could include completed patient registration forms if you emailed them to us, prescription or lab requests, and the content of voicemail messages you have left for our office as they would be email transcribed to us for quicker response. (Jay Scott Berenter, MD)

Attribution 1 Publication: CA AG'soffice / MT AG's office / hhs.gov Author:
Article Title: Synergy Specialists Medical Group
Article URL: https://oag.ca.gov/system/files/Q702_v01_Standard_Notice%201_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170127-01	International Code Council	DC	1/27/2017	Electronic	Business	Yes - Published #	11,177

On December 16, 2016, we discovered an issue potentially impacting the processing of credit and debit card purchases made through our online store. We immediately took action to secure our system and conducted an investigation to determine what information may have been accessed. The independent forensics investigation, which took time, determined that customer payment card information, including name, address, and credit/debit card information may have been compromised between the dates April 25, 2016 – May 24, 2016, and July 11, 2016 - September 14, 2016. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NH AG' Author:
Article Title: International Code Council
Article URL: https://oag.ca.gov/system/files/ICC%20Notice%20only%20California%20AG%20Notification%20Letter%20-%20ICC_0.p

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170126-01	Tipton County School District	TN	1/24/2017	Electronic	Educational	Yes - Published #	700

A digital security breech has potentially put the Social Security numbers of Tipton County's largest employer in the hands of those with malicious intent.

Attribution 1 Publication: Covingtonleader.com Author:
Article Title: Data breach affects thousands of school system employees
Article URL: http://www.covingtonleader.com/news/data-breach-affects-thousands-of-school-system-employees/article_d03ad41e-e

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170123-04	South Washington County Schools	MN	1/20/2017	Electronic	Educational	Yes - Published #	3,250

South Washington County Schools is investigating after a student gained access to electronic personnel data. The district notified all of its roughly 3,250 employees last week that it discovered the data breach and was investigating with the help of law enforcement and a computer forensic firm.

Attribution 1 Publication: woodburybulletin.com Author:
Article Title: District 833, police investigate after student accesses private employee data
Article URL: http://www.woodburybulletin.com/news/education/4203338-district-833-police-investigate-after-student-accesses-priv

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170123-03	Argyle Independent School District	TX	1/20/2017	Electronic	Educational	Yes - Published #	500

Hundreds of employees in the Argyle Independent School District are at risk of having their identities stolen. This, after a scammer sent an email posing as the schools' superintendent and asking for personal information.
Nearly 500 current and past employees are affected, including everyone who worked for the district in any way in 2016. That includes substitutes and anyone else who would have a W-2 from the district.

Attribution 1 Publication: NBCDFW.com Author:
Article Title: Hundreds of Argyle ISD Employees at Risk for Identify Theft After Data Breach
Article URL: http://www.nbcdfw.com/news/local/Hundreds-of-Argyle-ISD-Employees-at-Risk-for-Identify-Theft-After-Data-Breach-41

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170123-02	Bowlmor AMF	VA	1/20/2017	Electronic	Business	Yes - Published #	1,335

Bowlmor AMF, the world's largest bowling center operator, said late Friday that it had a possible data breach at 21 of its more than 300 domestic locations in 12 states between Feb. 4 and March 19. The only information collected was credit card number, a cardholder's name and credit card expiration date, the company said. (Exposure number per NY AG's office / notification from Discover)

Attribution 1 Publication: Richmond Times-Dispatch / MD AG's off Author:
Article Title: Bowlmor AMF
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-278646.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170123-01	Ohio State Veterinary Medical Center	OH	1/20/2017	Electronic	Educational	Yes - Published #	4,611

A malware infection is to blame for a security breach that could put the personal information of up to 4,611 clients of the Ohio State Veterinary Medical Center at Dublin in jeopardy.

Attribution 1 Publication: thelantern.com Author:
Article Title: Ohio State Veterinary Medical Center at Dublin hit with possible data breach
Article URL: http://thelantern.com/2017/01/ohio-state-veterinary-medical-center-at-dublin-hit-with-possible-data-breach/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-27	University of Maryland School of Medicine	MD	1/13/2017	Electronic	Medical/Healthcare	Yes - Published #	1,320

A doctor's practice plan affiliated with the University of Maryland School of Medicine has notified patients that somebody hacked the account of a physician assistant's email account that contained the personal information of patients. The email account contained personal patient information, including full names, dates of birth, home addresses, medical record numbers, health insurance information, prescription information, and diagnosis or treatment information. The Social Security numbers of 12 patients were also in the email, but no credit card, banking or other financial information was obtained.

Attribution 1 Publication: databreaches.net / baltimoresun.com / h Author:
Article Title: Email account with patient information at UM doctors group hacked
Article URL: http://www.baltimoresun.com/news/maryland/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-26	Dracut Public Schools	MA	1/15/2017	Electronic	Educational	Yes - Unknown #	Unknown

Employees of Dracut Public Schools in Massachusetts weren't as fortunate as those at Kanawha County Schools in West Virginia. Rick Sobey and Todd Feathers report that current and former employees' personal information, including SSN, was acquired by a hacker after an employee fell for what the district describes as a "sophisticated phishing scheme."

Attribution 1 Publication: databreaches.net / NH AG's office Author:
Article Title: Dracut schools employee data hacked after employee falls for phishing attempt
Article URL: https://www.databreaches.net/ma-dracut-schools-employee-data-hacked-after-employee-falls-for-phishing-attempt/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-25	Little Red Door Cancer Services of East Central	IN	1/20/2017	Electronic	Business	Yes - Unknown #	Unknown

TheDarkOverlord has struck again, this time the victim was a small Indiana cancer charity. The attack occurred on January 11 and was accompanied with a 50 Bitcoin ($43,000) ransom demand. Little Red Door Cancer Services of East Central Indiana was threatened with the publication of confidential data if the ransom was not paid. The stolen data included documents pertaining to grants, donors, employees, and the organization's operations.

Attribution 1 Publication: databreaches.net / hipaajournal,com Author:
Article Title: Hacking Group Attempts to Extort Funds from Cancer Services Provider
Article URL: http://www.hipaajournal.com/hacking-group-attempts-extort-funds-cancer-services-provider-8657/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-24	MrExcel.com	FL	1/16/2017	Electronic	Business	Yes - Unknown #	Unknown

On or about January 8, 2017, we became aware of evidence suggesting that some user information had been acquired in the December 5 hack and had been posted online. The hacker accessed and posted userid, e-mail address, and the encrypted password in the form of hash+salt. The hacker also accessed and posted information from administrative fields showing your last login, number of posts and similar non-personally identifiable information. If you had an account at the MrExcel Message Board on or before December 6, 2016, you are affected.

Attribution 1 Publication: databreaches.net / company website Author:
Article Title: Details of Data Breach at MrExcel.com
Article URL: https://www.databreaches.net/details-of-data-breach-at-mrexcel-com/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-23	**PopEyes / CCC Restaurant Enterprises, LLC.**	LA	1/18/2017	Paper Data	Business	Yes - Unknown #	**Unknown**

On July 9, 2016, CCC Restaurant, doing business as POPEYES, began investigating some unusual activity reported to the company by its credit card processor. CCC Restaurant retained a third-party forensic expert to investigate this report and to identify any signs of compromise on its systems. CCC Restaurant discovered evidence on its computer systems that indicated a potential compromise of customers' debit and credit card data for some debit and credit cards used at certain CCC Restaurant locations.

Attribution 1 Publication: databreaches.net / MD AG's office / NY Author:
Article Title: POPEYES discloses payment card breach that began in May, 2016; 10 locations affected
Article URL: https://www.databreaches.net/popeyes-discloses-payment-card-breach-that-began-in-may-2016-10-locations-affected/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-22	**Interpreters Unlimited**	CA	1/19/2017	Electronic	Business	Yes - Published #	**619**

A California-based translation and interpreter company has confirmed a massive data exposure, which if abused could have let hackers raid the company's systems and email accounts, and ransack other sensitive corporate and financial information. The files also contained highly sensitive private data of clients, employees and new hires, which included names, addresses, phone numbers, and Social Security numbers. (Exposure number per NY AG's office)

Attribution 1 Publication: MD AG's office Author:
Article Title: Interpreters Unlimited
Article URL: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280659%20(2).pdf

Attribution 2 Publication: databreaches.net / ZDNet.com / VT AG' Author:
Article Title: California translation firm's security lapse exposes sensitive files
Article URL: http://www.zdnet.com/article/california-translation-firms-security-lapse-exposes-sensitive-files/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-21	**Complete Wellness**	MD	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	**600**

The warning described an incident in which an employee – without authorization – copied patient files to a flash drive, and the flash drive was then lost. The incident affected 600 patients of two of the center's providers. We have learned that the personal information you provided in you initial paperwork, including name, address, phone numbers, email address, birthdate, age, social security number, languages spoken, emergency contact, level of education, employer information, primary care physician, list of medications at admission, list of allergies, ethnicity, race, marital status, hurricane victim status, living situation, military service, arrest history, and hearing or vision difficulties, may have been compromised.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Complete Wellness notifies 600 patients after employee misconduct results in lost PHI
Article URL: https://www.databreaches.net/md-complete-wellness-notifies-600-patients-after-employee-misconduct-results-in-lost-

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-20	**Catholic Charities of Baltimore (Associated**	MD	1/20/2017	Electronic	Business	Yes - Published #	**1,145**

We learned on November 29, 2016, that a Catholic Charities employee's email mailbox was accessed by unknown person(s) without authorization on October 17, 2016. While we have no evidence that the unknown person(s) actually read the emails, we are notifying individuals of the incident out of an abundance of caution. We are not aware of any fraud or misuse of any information as a result of this incident.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Catholic Charities of Baltimore Notifies Clients of Potential Security Incident
Article URL: https://www.databreaches.net/catholic-charities-of-baltimore-notifies-clients-of-potential-security-incident/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-19	Center for Mental Health	MT	1/19/2017	Paper Data	Medical/Healthcare	Yes - Unknown #	Unknown

On November 29, 2016, we learned that a document containing your name, Social Security number, date of birth, and limited health information was found outside the residence of a C4MH client by a nine-year old girl and given to a police offic.er. The officer returned the document to us. We immediately conducted an investigation into how the list could have been lost and determined that one of our employees, who was doing a medication delivery to the housing complex, had been in possession of the list and it likely fell out of their car.

Attribution 1 Publication: MT AG's office Author:
Article Title: Center for Mental Health
Article URL: https://dojmt.gov/wp-content/uploads/Center-for-Mental-Health.pdf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-18	Contech Engineered Solutions	OH	1/17/2017	Electronic	Business	Yes - Unknown #	Unknown

On October 10, 2016, we learned that password-protected laptop computers issued to our employees had been stolen from our Irving, Texas facility. The theft was reported to the Irving Police Department, and we immediately began an internal investigation. After conducting a thorough review, we determined that one of the laptops contained your name, address, and driver's license number. Although we continue to work with law enforcement, at this time, the laptops have not been located.

Attribution 1 Publication: MT AG's office Author:
Article Title: Contech Engineered Solutions
Article URL: https://dojmt.gov/wp-content/uploads/Contech-Engineerd-Solutions.pdfhttps://dojmt.gov/wp-content/uploads/Contech

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-17	Spiraledge, Inc. / SwimOutlet.com	CA	1/20/2017	Electronic	Business	Yes - Published #	426,623

On October 31, 2016, we began investigating some unusual activity reported by our credit card processor. We immediately began to work with third-party forensic experts to investigate these reports and to identify any signs of compromise on our systems. On November 28, 2016, we received confirmation of a sophisticated cyberattack in which a hack into our system may have compromised some customers' debit and credit card data used at www.swimoutlet.com between May 2, 2016-November 22, 2016. The information at risk as a result of this event includes the cardholder's name, address, phone number, email address, card number, expiration date, and CVV. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NH AG' Author:
Article Title: Spiraledge, Inc. / SwimOutlet.com
Article URL: https://oag.ca.gov/system/files/Spiraledge%20CA%20Form%20Exhibits%20A%20and%20B%20NON-MASS_RI_Sample

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-16	Children's Hospital Los Angeles	CA	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	3,594

On December 21, 2016, we learned that a laptop that was stolen from the locked vehicle of a Children's Hospital Los Angeles Medical Group physician who practices at Children's Hospital Los Angeles was unencrypted. The laptop may have had files on it with your child's name, date of birth, address, medical record number and some clinical information.

Attribution 1 Publication: CA AG'soffice Author:
Article Title: Children's Hospital Los Angeles
Article URL: https://oag.ca.gov/system/files/CHLA.Minor_.PHI_.011317.SAMPLE_0.pdf?

Attribution 2 Publication: databreaches.net / hhs.gov Author:
Article Title: Children's Hospital Los Angeles and the Children's Hospital Los Angeles Medical Group notify parents of laptop theft
Article URL: https://www.databreaches.net/childrens-hospital-los-angeles-and-the-childrens-hospital-los-angeles-medical-group/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-15	CoPilot Provider Support Services, Inc.	NY	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	221,178

Today, CoPilot Provider Support Services, Inc. (“CoPilot”) announced it has been made aware of and managed an unauthorized access of one of its databases used by healthcare professionals and notified patients whose information may have been included in the impacted database. Although CoPilot does not have evidence to suggest that any patient information was distributed or misused for purposes of identity theft or to cause financial harm, CoPilot has proactively notified patients out of an abundance of caution. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / databreaches.net / NY Author:
Article Title: CoPilot Provider Support Services notifies 220,000 of data security breach in 2015
Article URL: https://www.databreaches.net/copilot-provider-support-services-notifies-220000-of-data-security-breach-in-2015/

Attribution 2 Publication: govinfosecurity.com / MD AG's office Author: Marianne Kolbasuk M
Article Title: Unauthorized Access Breach Raises Many Questions
Article URL: http://www.govinfosecurity.com/unauthorized-access-breach-raises-many-questions-a-9645

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-14	Department of Justice	CA	1/20/2017	Electronic	Government/Military	Yes - Published #	3,424

On October 14, 2016, during the course of responding to a California Public Records Act for information pertaining to Certified California Firearm Safety Instructors, the Department inadvertently released your name, date of birth, California Drivers License number,nd California Identification Card number.

Attribution 1 Publication: CA AG's office Author:
Article Title: Department of Justice
Article URL: https://oag.ca.gov/system/files/NEW_EXPERIAN_C5147_FINAL%20NOTIFICATION%20LETTER%2012%2020%2016%20

Attribution 2 Publication: databreaches.net Author:
Article Title: California snafu releases personal info of nearly 4,000 gun safety instructors
Article URL: https://www.databreaches.net/california-snafu-releases-personal-info-of-nearly-4000-gun-safety-instructors/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-13	PathGroup	TN	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	1,443

PathGroup TN Health Plan 1443 12/29/2016 Unauthorized Access/Disclosure Other

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-12	Humana Inc. #HU16004F3	KY	1/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	3,674

Humana Inc. [case #HU16004F3] KY Health Plan 3674 12/19/2016 Unauthorized Access/Disclosure Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Humana Inc. #HU16004F3
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-11	MetroPlus Health Plan	NY	1/3/2017	Electronic	Medical/Healthcare	Yes - Published #	808

MetroPlus Health Plan NY Health Plan 808 01/03/2017 Unauthorized Access/Disclosure Other

Attribution 1 Publication: hhs.gov Author:
Article Title: MetroPlus 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
ITRC20170120-10	American Urgent Care Center, PSC	KY	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	822

The covered entity (CE), American Urgent Care Center, PSC, discovered that, upon her resignation, a former employee took an x-ray logbook on October 28, 2016. The log book contained the names and treatment dates of 822 individuals.

Attribution 1 Publication: hhs.gov Author:
Article Title: American Urgent Care Center, PSC
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-09	Office of Dr. David Elbaum	CA	1/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	500

Office of Dr. David Elbaum CA Healthcare Provider 500 01/09/2017 Theft Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-08	Offices of Bryan Myers, Ashley DeWitt and Michael	TN	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	13,150

Bryan Myers, MD PC, Ashley DeWitt, DO PC, Michael Nobles, MD PC TN Healthcare Provider 13150 12/30/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Offices of Bryan Myers, Ashley DeWitt and Michael Nobles
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-06	Office of Stephen J. Helvie, MD	CA	1/20/2017	Paper Data	Medical/Healthcare	Yes - Published #	2,013

Stephen J. Helvie, M.D. CA Healthcare Provider 2013 12/22/2016 Theft Paper/Films

Attribution 1 Publication: hhs.gov Author:
Article Title: Office of Stephen J. Helvie, 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
ITRC20170120-05	Waiting Room Solutions LLP	NY	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	700

Waiting Room Solutions LLP NY Business Associate 700 12/23/2016 Unauthorized Access/Disclosure Email

Attribution 1 Publication: hhs.gov Author:
Article Title: Waiting Room Solutions 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
ITRC20170120-04	PrimeWest Health / Summit Reinsurance Services, Inc.	MN	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	2,441

Based on the investigation, it looks like the unauthorized computer access first happened on March 13, 2016, according to PrimeWest leaders. To date, however, there is no evidence that member data was used inappropriately. The information on the affected server may have included members' names, Social Security numbers, health insurance information, providers' names and/or medical records.

Attribution 1 Publication: hhs.gov / echopress.com Author:
Article Title: PrimeWest Health
Article URL: http://www.echopress.com/news/4204344-primewest-reports-possible-security-breach

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-03	Henry County Health Department	OH	1/20/2017	Electronic	Government/Military	Yes - Published #	574

Henry County Health Department OH Healthcare Provider 574 12/21/2016 Theft Electronic Medical Record, Email, Laptop, Paper/Films

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

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170120-02	Brodhead Dental Center	PA	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	5,872

Brodhead Dental Center PA Healthcare Provider 5872 12/19/2016 Hacking/IT Incident Desktop Computer

Attribution 1 Publication: hhs.gov Author:
Article Title: Brodhead Dental 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
ITRC20170120-01	Alliant Health Plans, Inc.	GA	1/20/2017	Electronic	Medical/Healthcare	Yes - Published #	Unknown

Alliant Health Plans, Inc. GA Health Plan 1042 12/20/2016 Hacking/IT Incident Network Server

Attribution 1 Publication: hhs.gov Author:
Article Title: Alliant Health Plans, Inc.
Article URL: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170117-01	Sentara Healthcare	VA	1/16/2017	Electronic	Medical/Healthcare	Yes - Published #	5,454

Sentara Healthcare said Monday that a "cybersecurity incident" involving one of its third-party vendors affected the records of more than 5,000 patients. The accessed information may have included patients' names, medical record numbers, dates of birth, social security numbers, procedure information, demographic information and medications.

Attribution 1 Publication: abc13newsnow.com / hhs.gov Author:
Article Title: Security breach affected thousands of Sentara Healthcare patients
Article URL: http://www.13newsnow.com/news/health/security-breach-affected-thousands-of-sentara-healthcare-patients/38652216

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170113-02	Highmark Blue Cross Blue Shield of Delaware / Summit	DE	1/13/2017	Electronic	Medical/Healthcare	Yes - Published #	19,000

On August 8, 2016, Summit discovered that ransom ware had infected a server containing certain personal information. The information contained on the affected server may have included your name, Social Security number, health insurance information, provider's name, and/or claim-focused medical records containing diagnosis and clinical information.

Attribution 1 Publication: First State Update Author:
Article Title: Delaware Data Breach Affects 19,000
Article URL: http://firststateupdate.com/2017/01/delaware-data-breach-affects-19000/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170110-06	Los Angeles Valley College	CA	1/8/2017	Electronic	Educational	Yes - Published #	1,900

Los Angeles Valley College was the victim of a ransomware hacking attack that took down the campus's website and email system on New Year's Day until the school paid $28,000 to free hostage data. 1,900 students and faculty were locked out of their computers with the message: "You have 7 days to send us the BitCoin after 7 days we will remove your private keys and it's impossible to recover your files," according to the campus newspaper.

Attribution 1 Publication: breitbard.com Author:
Article Title: LA College pays $28K Ransom to Free Student, Faculty Data
Article URL: http://www.breitbart.com/california/2017/01/08/la-college-pays-28k-ransom-free-student-faculty-data/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170110-05	Susan M. Hughes Center	NJ	1/10/2017	Electronic	Medical/Healthcare	Yes - Published #	11,400

On August 30, 2016, we became aware of a ransomware attack of our computer system. We immediately began an investigation, reset passwords, removed the server from the system, and began using back up to our system. We engaged a leading forensic firm to assist in the investigation and we determined that an unknown person remotely accessed a server which contained files that may have included patients' names, telephone numbers, dates of service, types of service or treatment, and amounts paid.

Attribution 1 Publication: databreaches.net / hhs.gov Author:
Article Title: Susan M. Hughes Center
Article URL: https://www.databreaches.net/cosmetic-surgery-center-discloses-ransomware-attack/

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170110-04	E-Sports Entertainment Association (ESEA)	NJ	1/8/2017	Electronic	Business	Yes - Unknown #	Unknown

E-Sports Entertainment Association (ESEA), one of the largest competitive video gaming communities on the planet, was hacked last December. As a result, a database containing 1.5 million player profiles was compromised.

Attribution 1 Publication: eSecurityPlanet.com / databreaches.net Author:
Article Title: ESEA Hacker Demands $100,000, Exposes 1.5 Million User Records
Article URL: http://www.esecurityplanet.com/hackers/esea-hacker-demands-100000-exposes-1.5-million-user-records.html

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170110-03	Unison Home / R&A Design	IL	1/10/2017	Electronic	Business	Yes - Published #	1,500

At some point between May 16, 20 16 and August 6, 20 16, malicious code was placed on Unison Home's website at vvww.unisonhome.com (the "Website"). From that time until October 18, 2016, that malicious code was able to access customers' names, shipping and billing addresses, telephone numbers, credit card information (credit card numbers, security codes, and expiration dates), email addresses, and account passwords (for Unison Home online account holders) when Website users entered that information on the Website. (Exposure number per NY AG's office)

Attribution 1 Publication: VT AG's office / NH AG's office / ME AG' Author:
Article Title: Unison Home / R&A Design
Article URL: http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Unison%20Home%20-%20R&A%20Design%20SBN%20

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170110-02	Office of Kevin Harrington, CPA	CA	1/9/2017	Electronic	Business	Yes - Unknown #	Unknown

On November 11, 2016, I detected that someone may have accessed my computer without authorization. The following information appears to have been accessed: tax return information which included names, addresses, dates of birth, and Social Security numbers.

Attribution 1 Publication: CA AG's office / NH AG's office Author:
Article Title: Office of Kevin Harrington, CPA
Article URL: https://oag.ca.gov/system/files/Consumer%20Notification%20Letter%20%28Kevin%20Harrington%29_0.pdf?

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20170110-01	**Legal Aid Society of Orange County**	CA	1/6/2017	Electronic	Business	Yes - Published #	**1,239**

On October 31, 2016, LASOC became aware that certain completed tax forms from the 2007 and 2008 tax years had become temporarily accessible to the general public through a directed search on certain internet search engines. As part of the investigation into this incident, LASOC determined a tax form containing the following information about you, as provided by the filer, was temporarily accessible to the general public through a directed search on certain internet search engines: name and Social Security number. (Exposure number per NY AG's office)

Attribution 1 Publication: CA AG's office / MT AG's office / NY AG' Author:
Article Title: Legal Aid Society of Orange County
Article URL: https://oag.ca.gov/system/files/Legal%20Aid%20Orange%20County%20NOTICE_0.pdf?

2017 Breaches Identified by the ITRC as of:	1/19/2018

Total Breaches:	1,579
Records Exposed:	178,955,069

The ITRC Breach database is updated on a daily basis, and published to our website on Tuesday. Unless noted otherwise, each report includes breaches in the U.S. that occurred in the year of the report name (such as "2017 Breach List"), or became public in the report name year, but were not public in the previous year. For any breach which may have a corporate office outside of the U.S., but has customers in the U.S., the breach location will be identified as US. 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.

CYBERSCOUT Formerly IDT911

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