

Data Breach Self-Protection Guide

10 Steps for Consumers and 7 Steps for Businesses to Protect Themselves Against Data Compromise Before- & After-the-Fact

On September 7, 2017, the Equifax breach that impacted close to 150 million American households was publicly revealed. Ever since, news articles have continued cycling, initially providing explanations of how the hack occurred, expressing the frustration and anger of consumers, and explaining their changing offers to manage the risks posed to all the consumers whose data was stolen. Later, indictments came for insider trading related to the breach, as well as an agreement with eight US states where Equifax promised to beef up its security in exchange for avoiding steep fines. In the year since the breach, we've seen many more data breaches not only continue to occur but accelerate. In the enclosed list of 2017–2018 data breaches starting on page 4 of this guide, we exceeded the number of data breaches in the first half 2018 that we saw in all of 2017. The unfortunate reality is this trend is going to continue so businesses and consumers need to continue stepping up practices to protect applications and data from theft, as well as have a plan in place if that data is stolen.

The remainder of this Guide provides steps to help you do just that.

10 Steps You as a Consumer Can Take to Protect Your Identity, Credit and Personal Information

- 1. Check the status of your data.** It's not too late to find out if your information was stolen in the Equifax breach. Go to www.equifaxsecurity2017.com and follow the prompts. You'll be asked to enter your last name and the last 6 digits of your social, which is a bit painful as normally you're only asked to provide the last 4 digits. There's a good chance your information was stolen in this breach so it's worth checking.

If you were fortunate enough to sidestep this data breach, your data could still be at risk from any of the other breaches in recent months/years. Experian offers a free search to find out if your information is on the dark web, along with other scans offered by various credible vendors. If you're up for it, the Experian search can be done here: www.experian.com/consumer-products/free-dark-web-email-scan.html or also simply www.experian.com/scan.

- 2. Accept free monitoring.** If your Equifax, Experian or other search results indicate your information may have been stolen, take advantage of any free monitorings offered by the company who housed your information. While monitoring alone and only for one year is not enough, it keeps you informed and covers that much time while you put some other safeguards in place.

3. Freeze your credit. Based on a recent signing of a bill by Congress (<https://virsec.com/credit-freezes-will-soon-be-free-to-consumers>), credit freezing will soon be free. This may be even more important than Step 2 because credit monitoring won't stop hackers from using your information to steal your identity, it will only tell you after they've made an attempt or have already successfully done it. A credit (aka security) freeze blocks activity and use of your information. The previous cost to set a credit freeze was in the range of \$6–\$10 per credit company, but by the time you are reading this, the fees may already be a thing of the past.

To access Equifax's credit freeze option, go to www.freeze.equifax.com. You can also send a request in writing to Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348. You'll need to send specific personal information so refer to the website noted above.

Please be aware that a credit/security freeze with Equifax does not effect your information with the other two primary credit companies, Experian or TransUnion, so to be fully covered, freezes would be needed at all three. Once they are free, that will be an easier task. And last, be aware that such a freeze prevents businesses from performing credit activities, such as credit checks, on your information so if you actually want such actions performed, you would need to lift the freeze(s) via use of a PIN or some security measure you would provide to unlock the information in specific situations. (Some headache is involved for consumers but far less than having your identity stolen to be sure.)

4. Establish a baseline. Check your credit report to establish a “before” baseline.

5. Enroll in additional free credit score services. You can find 8 of them here: www.consumerismcommentary.com/free-credit-score

6. Manage your passwords responsibly. Take inventory of your account passwords, especially at banks and financial institutions. Change your passwords often and use something other than your kiddo's birthday or your pet's name. Don't use the same password (or slight variations) for multiple accounts. Make it complicated—a pain to remember so you may want to get a password keeper or manager to keep track of them safely (just Google 'password manager' for a list of options to evaluate).

7. Use two-factor authentication. Take advantage of two-factor authentication when it's offered in your accounts, designed to ensure that hackers won't have at least one of those factors and be denied access. It has been documented that two-factor authentication is an effective deterrent against identity theft.

8. Be vigilant in confirming all sources of all email communication. Be suspicious of every communication (email, text, snail mail) that appears to come from Equifax or other entities claiming to offer information or assistance. Always confirm authenticity before taking any action or providing any information.

9. Watch your accounts. Monitor your accounts regularly to spot any unauthorized charges or activity.

10. Learn and protect your rights. Keep your options open by protecting your rights. Don't agree to any vendor offerings that are associated with terms that could compromise your rights. Initially Equifax's free credit monitoring came with restricting class action terms but these were disputed and removed.



7 Steps Your Business Can Take to Protect Your Company Web Servers, Applications and Information

In our current era of continual cybersecurity threats, having proactive protective mechanisms in place could not be more critical. A couple basics are always standard best practices:

1. **Backups:** Perform daily backups of important data including project logic, configuration files and application installers.
2. **Patching:** You're better off applying patches promptly (keeping in mind that this won't stop zeroday exploits).

The above steps alone are not nearly enough so below are some additional best practices we recommend for any organization concerned about avoiding their own disastrous data breach:

3. **Be situationally aware:** Watch CERT databases, vendor and OS advisories, and subscribe to hacker channels.
4. **Perform regular vulnerability scans:** Keep an eye out for internal configurations that can lead to leaks.
5. **Organize war games:** Red-Blue Team simulations can often lead to surprising and useful discoveries.
6. **Monitor data traffic:** Track daily and hourly data extraction for all users and look for anomalies.
7. **Protect apps at the process memory level:** Use pro-active control flow technology like Virsec's Trusted Execution to protect all critical applications.

It's this last point especially that could have and would have prevented Equifax's breach, even without the patch they could have applied. Instead of being in reactive mode trying to bop every threat that pops up like some kind of losing round of Whack-a-Mole, Virsec's Trusted Execution takes a completely different approach to protecting web servers and applications.

By understanding an application's DNA, any bad behavior is instantly detected in ways other technologies continue to miss. In a data breach like Equifax, had their web servers been protected by Virsec, the attacks that exploited the Apache Struts Vulnerability CVE 2017-9805* would have been spotted in real time at multiple points, and quickly stopped before damage was done and sensitive information stolen. If only.

Virsec's unique approach provides preemptive protection against these kinds of attacks, fileless attacks, memory-based attacks and more. To learn more about Virsec's unique solution, check out these blogs:

To learn more about Virsec's unique solution, check out these blogs:

[Behind the Equifax Breach: Apache Struts Vulnerabilities, Laxed Patching and Zero-Day Exploits](#)

[Protection Against Advanced Web Attacks](#)

[Spectre and Meltdown Attack Prevention](#)

[Keeping the Lights on in the era of critical infrastructure attacks](#)

[Virsec Hack Analysis Deep Dive into Industroyer aka Crash Override](#)

[Talk to us or request a demo](#)

* Pinpointed and identified by Virsec Founder Satya Gupta even before it was publically acknowledged—watch his [video interview](#) and read his [technical deep dive blog](#).



Significant Data Breaches (2017–2018)

Timeline of Major Breaches in 2018

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
1	January 8, 2018	2+ years ago	Vtech	6.4 million children	Personal data including name, gender, birth date and more without parent permission; will pay \$650,000
2	January 11, 2018	2017	Jason's Deli	2 million data cards	Through access of point-of-sale terminals, cardholder name, credit or debit card number, expiration date, card holder verification value and service code were stolen and sold on dark web
3	January 17, 2018	Not specified	Aetna	12,000 members	Low-tech mailing error resulting in violation of privacy of HIV patients, Aetna to pay \$17 million in settlement
4	February 2, 2018	Not specified	CarePlus	11,200 members	Low-tech mailing error resulting in violation of privacy, disclosing information including member name, CarePlus identification number and plan name, dates of service, provider of service, and services provided
5	February 5, 2018	May 2017	Partners Healthcare	2,600 patients	Social Security numbers and financial data, second breach for this company
6	February 15, 2018	Between 2014–2017	FedEx	119,000 customers	Breach occurred through exposed AWS cloud server, revealing information included passports, drivers' licenses, names, home addresses, phone numbers and ZIP codes
7	March 12, 2018	May 2017–January 2018	BJC Healthcare	33,420 patients	Scanned images of documents revealed patient information

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
8	March 13, 2018	January 8, 2018	St. Peter's Surgery & Endoscopy Ctr.	134,512 individuals	Patient names, dates of birth, addresses, dates of service, diagnosis codes, procedure codes, insurance information, and, for those with Medicare, Social Security numbers
9	March 20, 2018	January 2016–December 2017	Orbitz, subsidiary of Expedia	880,000 customers	Personal information includes birthdays, addresses, full names, phone numbers, email addresses and gender
10	March 22, 2018	This year	ATI Physical Healthcare	35,136 patients	Email accounts containing sensitive patient information, including Social Security numbers, driver's license numbers, financial account numbers, Medicare or Medicaid ID numbers, and medical records
11	March 23, 2018	Not specified	Massive hack sponsored by Iran	144 US universities, plus American companies and government agencies	Email accounts of roughly 4,000 professors. Once inside, they stole 31 terabytes of intellectual property, totaling \$3.4 billion worth of damage
12	March 29, 2018	Not specified	Under Armour (MyFitnessPal)	150 million MyFitnessPAL users	Username, email addresses, and hashed passwords in one of largest cyberattacks on record
13	April 1, 2018	Began May 2017	Saks Fifth Avenue, Lord & Taylor	5 million cards	Data of credit and debit cards, one of the largest cyberattacks against a retailer so far
14	April 2, 2018	Began August 2017	Panera Bread	37 million customers	Full name, email and physical address, phone number, birthday, and last four digits of credit or debit card
15	April 16, 2018	January 2–March 14, 2018	Inogen	30,000 current & former customers	Includes names, telephone numbers, email addresses, dates of birth, dates of death, Medicare identification numbers, insurance policy information, and the type of medical equipment the company provided
16	April 20, 2018	November 1, 2017–February 7, 2018	Unity Point Health	16,000 people	Through email, patient Social Security numbers and financial information
17	April 20, 2018	Not specified	SunTrust Banks	1.5 million clients	Customers' names, addresses, phone numbers, and account balances
18	May 9, 2018	Not specified	City of Goodyear	30,000 utility customers	Fraudulent activity occurred on bank accounts
19	May 12, 2018	March & April 2018	Chili's	not known	Customers' credit and debit cards
20	May 14, 2018	November 2017–February 2018	Rail Europe	not specified	Customers' credit card numbers, expiration dates, CVV codes, name, gender, address, telephone number, email address, username and password
21	May 17, 2018	Not specified	Nuance Communications	45,000 patients	Patient names, dates of birth, medical record numbers, and information about their medical condition and treatments
22	May 21, 2018	Not specified	University at Buffalo	2,500 alumni, students, staff	Login information

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
23	May 22, 2018	September 2017	LifeBridge Health	500,000 patients	Names, addresses, birth dates, insurance information, and Social Security numbers
24	May 29, 2018	Not specified	Aultman Health Foundation	42,600	Email accounts revealing patient demographics, physical exam information, medical history, test results, and, for some, Social Security and driver's license numbers
25	June 3, 2018	Not specified	Ticketfly	26 million customers	Included customer names, addresses, email addresses, and telephone numbers
26	June 5, 2018	Not specified	MyHeritage	more than 92 million people	Email addresses and hashed passwords
27	June 7, 2018	Not specified	Dignity Health	55,947 patients	Misaddressed emails exposed personal information of patient names and name of physician
28	June 11, 2018	June 11, 2018	Coinrail	up to 30% of coins in storage—\$37.2M	South Korean cryptocurrency stolen, worth \$37.2M and causing other cryptocurrency values to plummet
29	June 17, 2018	June 17, 2018	Chicago Public Schools (CPS)	3,700 families	Employee accidentally emailed private info to > 3,700 families; names, email addresses, phone numbers and student IDs
30	June 20, 2018	June 20, 2018	Bithumb	\$32 million	2nd major cryptocurrency heist of the month—see Coinrail above
31	June 21, 2018	June 21, 2018	Med Associates	270,000 patients	Employee workstation compromised by third party; patient info stolen including names, DOB, diagnosis codes & insurance info
32	June 25, 2018	June 25, 2018	Task Rabbit	3.75 million users	A freelance labor for hire website breached by hacker who targeted names, DOB, SS#, and bank account numbers of customers and labourers; 12 months of free identity restoration services offered
33	June 25, 2018	June 25, 2018	Click2Gov—Midwest City	2,300 users	Customer names, billing addresses, payment card info
34	June 27, 2018	June 27, 2018	Exactis	340,000 million records=230,000 consumer info, 110,000 business	One of the largest breaches in history, server left unprotected on publicly accessible server; info stolen was consumer PII including phone numbers, addresses, email addresses, many of 400 other of variables on the individuals
35	June 27, 2018	June 27, 2018	Ticketmaster	unknown # of event goers	"Magecart" hackers altered website code and skimmed credit card data entered at checkout; 800 other sites affected by similar attacks
36	June 30, 2018	prior to June 30, 2018	Adidas	millions of online customers	Contact information, usernames, and encrypted passwords taken off Adidas website
37	July 7, 2018	July 7, 2018	Timehop	21 million users	Names and emails of all its users, 4.7 million of whom also had a phone number exposed; Timehop has taken steps to add multifactor authentication to its cloud security

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
38	July 9, 2018	time prior to July 9, 2018	Polar Fitness Trackers		Highly sensitive personal and geographical information of military and counter intelligence personnel from leak on Polar Flow social platform; fitness & GPS tracking information that would give holders of that info location knowledge of military bases, embassies, airfields, nuclear storage sites, and intelligence agencies. Users of the tracking apps advised to enable all available privacy settings and be diligent of online forum information available about them
39	July 10, 2018	April 26–June 12, 2018	Macy's	Online shoppers at Macy's during this period	Names, phone numbers, email addresses, birth dates, and credit and debit card numbers with the expiration dates; noted as one of many breaches against retailers
40	July 11, 2018	prior to July 11, 2018	US Air Force	captain's computer with drone data	Military data breached by amateur hacker into a captain's computer, taking classified information and documents about MQ-9A Reaper drones and their operators; the hacker tried to sell the information on the Dark Web for \$150
41	July 11, 2018	July 11, 2018	Nashville Metro Public Health	thousands of HIV patients	PII of HIV patients on server including names, addresses, SS#s, DOBs, sexual preferences, illegal drug use history and more; data could have been accessed by more than 500 Metro employees
42	July 12, 2018	July 12, 2018	UMC Physicians (UMCP)	18,000 patients	Email accounts hacked, exposing names, addresses, phone numbers, medical record numbers, diagnoses, SS#s, DOB, and health insurance information; UMCP patients offered 1 year of free monitoring and ID theft protection
43	July 17, 2018	prior to July 17, 2018	LabCorp Diagnostics	undisclosed	RDP brute-force attacks installed SamSam ransomware to extort info
44	July 20, 2018	prior to July 20, 2018	Boys Town National Research Hospital	105,309 patients and employees	Another email account hacked gave access to patient and employee names, DOBs, SS#s, Medicare or Medicaid ID numbers, treatment information, medical record numbers, billing information, and health insurance information
45	July 20, 2018	prior to July 20, 2018	ComplyRight Tax Prepayer	662,000 people	Names, addresses, phone numbers, email addresses, and SS#s; 12 months of free credit monitoring offered to victims
46	July 25, 2018	prior to July 25, 2018	LifeLock	millions of customers	Customer email addresses, allowing anyone to manipulate customer accounts
47	July 31, 2018	prior to July 31, 2018	Unity Point Health (2)	1.4 million patients	Through a phishing attack, information stolen included health information, names, addresses, medical data, insurance information, and possibly payment card and SS#s; 2nd breach this year for Unity and largest healthcare breach of the year
48	August 1, 2018	from 2007	Reddit	users from 2007	Current email addresses, and passwords from 2007, outdated two-factor authentication, patients advised to change passwords

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
49	August 3, 2018	between March 2017–July 2018	TCM Bank	10,000 credit card applicants	Names, addresses, DOBs and SS#s
50	August 7, 2018	prior to August 7, 2018	SSM Health St Mary's Hospital	301,000 patients	Documents and other materials with patient health information discovered at former site set for demolition
51	August 10, 2018	January 1, 2013–March 28, 2018	Adams County, WI	258,120 individuals	Names, addresses, personal information, photographs, health, and tax information
52	August 14, 2018	prior to August 14, 2018	MedSpring Urgent Care	13,000 patients	Through a phishing attack, stolen information includes patient names, account numbers, medical record numbers, dates of medical services received
53	August 15, 2018	prior to August 15, 2018	Instagram	thousands of photo app users	Hackers changed the contact information linked to accounts, making it extremely difficult for users to regain access; most cases involved email changing to .ru domain
54	August 16, 2018	prior to August 16, 2018	Augusta University	417,000 patients	Through a phishing attack, several email accounts of patients compromised in over 80 outpatient clinics
55	August 17, 2018	prior to August 17, 2018	Fortnite video game	undisclosed children players	Children's personal data for sale on the Dark Web, allowing scammers to buy credentials to not only rack up huge in-play charges in the video game but also gain access to bank accounts and payment card info; parents should closely monitor children's accounts
56	August 17, 2018	1998–2010 (students) & 2008–2018 (workers)	Eastern Maine Community College (EMCC)	42,000 people consisting of students & workers	Malware compromised EMCC and stole usernames, passwords, names, addresses, Social Security numbers, and dates of birth of 42,000 people may have been accessed.
57	August 20, 2018	prior to August 20, 2018	Legacy Health	38,000 patients	Through breached email account, personal, medical, and billing information stolen including patient names, DOBs, health insurance information, billing information, medical records, SS#s, and driver's license information
58	August 21, 2018	prior to August 21, 2018	Animoto	undisclosed video service users	Users' names, usernames, email addresses, hashed passwords, geolocation, gender, and DOB; no payment info
59	August 22, 2018	between November 2017–January 2018	Cheddar's Scratch Kitchen	567,000 restaurant customers	Credit card information, the restaurant owner, Darden, has replaced the compromised system
60	August 23, 2018	August 23, 2018	Sitter	93,000 Sitter users	Personal data exposed on an unsecured server: phone numbers, addresses, transaction details, phone contacts, partial credit card numbers, and encrypted account passwords
61	August 27, 2018	prior to August 27, 2018	T-Mobile	2 million customers	Hackers breached company system and stole customer names, billing zip codes, phone numbers, email addresses, account numbers, and account types. They've said no financial or billing data was compromised; users impacted were notified

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
62	August 29, 2018	prior to August 29, 2018	Air Canada	20,000 of 1.7 million mobile app customers	Names, email addresses, telephone numbers, Aeroplan numbers, passport information, and dates of birth; Air Canada locked down all accounts
63	September 4, 2018	the prior 6 months before September 2018	mSpy	all customers who logged in over the six months	Passwords, call logs, text messages, contacts, notes, and location data unprotected on an open database; 2nd breach in 3 years
64	September 5, 2018	prior to September 5, 2018	Orrstown Bank	over 50,000 bank customers	Customer information exposed through email accounts thanks to 2 employees falling for a phishing attack; company provided 2 years of free identity and credit monitoring
65	September 6, 2018	prior to September 6, 2018	Foosackly's	165,000 customers	the restaurant's payment system, compromising payment card data
66	September 7, 2018	between August 21–September 5, 2018	British Airways	380,000 customers on website or mobile app	Travelers who booked flights on the website or through mobile app between 8/21–9/5 were compromised, with stolen names, physical and email addresses, and full credit card details; British Airways to pay for credit checks and reimburse for any losses
67	September 17, 2018	records dating back to 2012	GovPayNow.com	over 14 million customers	Customer names, addresses, phone numbers, and partial credit card information was compromised
68	September 18, 2018	prior to September 18, 2018	MongoDB Server	11 million records	Names, email addresses, and physical addresses taken from an unprotected server, ownership still unknown, possibly an affiliate marketing program, SaverSpy
69	September 19, 2018	from August 14 to September 18	Newegg	not reported	Hacking group Magecart stole customer credit card info
70	September 19, 2018	prior to September 19, 2018	Independence Blue Cross	17,000 members	an employee uploaded protected health information onto a public-facing website; Blue Cross is offering 2 years of identity protection
71	September 25, 2018	began in June 2018, discovered in August	SHEIN	6.5 million shoppers	hackers targeted servers and stole customer email addresses and encrypted password credentials
72	September 26, 2018	April of 2018	Chegg	40+ million customers	customer names, email, physical addresses, usernames, and passwords. No Social Security or payment information was compromised; all 40 million passwords to be reset
73	September 28, 2018	discovered September 16	Facebook	90,000 million accounts	major invasion of privacy due to weakness in a line of code exposing a vulnerability in Facebook's "View As" feature
74	October 1, 2018	prior to October 1, 2018	Toyota	19,000 individuals	an infiltrated corporate email system revealed names, home addresses, dates of birth, phone numbers, financial information, Social Security numbers, and at least 12 additional types of sensitive data of the individuals
75	October 2, 2018	prior to October 2, 2018	Apollo	200 million contact records	Names, email addresses, company names, and other business contact information

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
76	October 3, 2018	prior to October 3, 2018	Central Maine Power	77,300	Improperly secured online letters revealed names, addresses, and former utility account numbers
77	October 8, 2018	bug from 2015 discovered in 2018	Google+	496,951 Google+ users	Undiscovered bug left user info accessible by developers, i.e., names, email addresses, dates of birth, gender, photos, location, occupation, and relationship status
78	October 14, 2018	prior to October 14, 2018	Department of Defense	30,000 employees or more	Hackers accessed a system with employee travel records, exposing personal and credit card info
79	October 19, 2018	found after suspicious activity in Direct Enrollment	US Centers for Medicare & Medicaid Services (CMS)	75,000	Files that were part of Direct Enrollment program, used by brokers helping consumers; type of data compromised not revealed
80	October 25, 2018	prior to October 25, 2018	Cathay Pacific	9.4 million people	Hong Kong-based airline breached revealing personal data, travel histories, phone numbers, dates of birth, frequent flier membership numbers, passport and government ID numbers, and email addresses; stock plummeted to 9 year low
81	October 25, 2018	registrations from 2003–2018	Jones Eye Clinic	40,000 people	Names, dates of birth, dates of service, medical record numbers, and social security numbers
82	October 26, 2018	October 24, 2018	Raley's	10,000 pharmacy customers	Due to a stolen laptop, names, genders, dates of birth, health plans, plan ID numbers, and medical conditions of pharmacy customers were stolen; law enforcement was notified
83	October 29, 2018	prior to October 29, 2018	Tomorrowland	64,000 EDM festival attendees in 2014	Personal information accessed through Paylogic ticketing system, including names, addresses, ages, postcodes, and genders
84	November 7, 2018	October 4–14, 2018	HSBC Bank	14,000 US customers	In a credential stuffing attack, names, addresses, phone numbers, email addresses, dates of birth, account numbers, account types, account balances, and transaction history exposed
85	November 8, 2018	prior to November 8, 2018	Canada Post	4,500 customers	Information accessed by Canada Post delivery tracking tool user, revealing names or initials, postal codes, dates of delivery, OCS reference numbers, tracking numbers, and OCS corporate names and business addresses
86	November 8, 2018	Since 2006	Huntsville Hospital	15,000 individuals	A vendor exposed application records containing personal information; hospital fired vendor and is providing identity theft protection
87	November 9, 2018	prior to November 9, 2018	Bankers Life	over 566,000 individuals	An unauthorized third party gained access to names, addresses, dates of birth, insurance information, and the last four digits of Social Security numbers; 5th largest breach reported to HIPAA Breach Reporting Tool in 2018
88	November 9, 2018	prior to November 9, 2018	Nordstrom	72,500 employees	A contractor at a retailer in Seattle accessed employee info, including names, Social Security numbers, dates of birth, checking account and routing numbers, salaries, and more; Nordstrom offered 2 years ID protection

► Timeline of Significant Data Breaches

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
89	November 12, 2018	between February–May 2018	Health First	42,000 customers	A few employees fell for a phishing scam leading to information compromise containing Social Security numbers, addresses, and dates of birth
90	November 12, 2018	prior to November 12, 2018	US Postal Service (USPS)	60,000 million people	Reported by CSO Online, the Secret Service alerted law enforcement that identity thieves broke into USPS Informed Delivery system. They signed victims up for credit cards, then stole the cards, along with email address, username, user ID, account number, street address, phone number, and tracking data.
91	November 16, 2018	prior to November 16, 2018	Vovox	26 million text messages	Security researchers discovered a vulnerability that exposed millions of private text messages, some containing password reset links, two factor authentication codes, and other data.
92	November 21, 2018	prior to November 21, 2018	Amazon	Unknown number of customers	Users received cryptic email saying their address was exposed due to technical error; Amazon didn't advise, but good advice to Amazon customers is to change their password
93	November 28, 2018	prior to November 28, 2018	Atrium Health	2.65 million patients	Caused by third party vendor AccuDoc, data exposed included names, addresses, dates of birth, insurance information, medical record numbers, and payment record as well as 700,000 social security numbers; those 700,000 were given free credit monitoring.
94	November 28, 2018	for 2 weeks prior to November 28, 2018	ElasticSearch	57 million Americans, possibly 26 million more	Data included names, email addresses, home addresses, states, ZIP codes, phone numbers, and IP addresses of 57 million, and a database of business information of 26 million more
95	November 29, 2018	prior to November 29, 2018	Dunkin' Donuts	Unknown number of Dunkin' Donuts loyalty members	Hacked information included names, email addresses, DD Perks account numbers, and DD Perks QR codes; Dunkin' Donuts issued a warning to customers who may have been affected.
96	November 30, 2018	going back to 2014	Marriott/Starwood	500 million guests	Starwood rewards information, travel details, and communication preferences of half a billion customers. An undisclosed number of guests also had their payment card numbers and expiration dates compromised.
97	December 3, 2018	in November or earlier	Signet Jeweler, owner of Kay and Jared jewelers	All online customers	In November of 2018 a customer noticed that by slightly modifying the confirmation link he received via email, he was able to see other customers' order details; compromised information included names, billing addresses, shipping addresses, phone numbers, email addresses, items purchased, delivery dates, tracking links, and the last four digits of credit card numbers.

► Timeline of Significant Data Breaches

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
98	December 4, 2018	prior to December 4, 2018	Quora	100,000 million users	Hacked information included users' names, email addresses, encrypted passwords, and publicly posted questions/answers/comments.
99	December 10, 2018	November 7	Google+ (second breach)	52.5 million users	An update to the Google+ API exposed users again for the second time; data included people's name, email address, occupation, and some additional profile information. After this second breach, Google+ has moved up its shutdown to April 2019.
100	December 10, 2018	October 31–December 7	City of Topeka, Utilities Dept	10,000 online paying residents	Online payment information
101	December 11, 2018	prior to December 11, 2018	Baylor Scott and White Medical Center—Frisco	48,000 patients	Payment information plus names, dates of service, medical record numbers, account data, insurance information, and invoice numbers.
102	December 14, 2018	12 days in September	Facebook	6.8 million users	A security bug allowed third-party app developers to view the private photos of 6.8 million users. Private photos, Facebook Stories, and Marketplace photos were exposed.
103	December 14, 2018	prior to December 14, 2018	Wright County, Minnesota	72,000 thousand people	An IT employee took private citizen information to work from home; Social Security numbers and financial information potentially compromised.
104	December 18, 2018	prior to December 18, 2018	University of Vermont Health Network—Elizabeth Town	32,000 patients and 1200 individuals	PII was exposed after an unauthorized individual gained control of an employee's email account, including names, dates of birth, addresses, medical information.
105	December 21, 2018	September–November 2018	Warby Parker	198,000 customers	Cybercriminals may have used stolen information, including usernames and passwords, obtained through security breaches at other companies; data included names, email addresses, last four digits of payment cards, and prescription information.
106	December 26, 2018	January–November 2018	San Diego Unified School District	500,000 staff and students	Through a phishing attack that 50 staff members fell victim to, the cybercriminal had access to school system going back to 2008–2009; data includes names, addresses, Social Security numbers, date of birth, phone numbers, payroll and compensation information, and health benefits enrollment information.
107	December 26, 2018	prior to December 26, 2018	BeMo!	14,000 customers	A hacker placed malicious code on the checkout page, capturing information including names, full credit and debit card details, billing addresses, shipping addresses, and telephone numbers.

Timeline of Major Breaches in 2017					
	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
1	January 8, 2017	December 30, 2016	E-Sports Entertainment Association (ESEA)	1,503,707 records	Private information including registration date, city, state, last login, username, first and last name, bcrypt hash, email address, date of birth, zip code, phone number, website URL, Steam ID, Xbox ID, and PSN ID
2	February 1, 2017	September 2015	Xbox 360 ISO & PSP ISO	2.5 million	Email addresses, usernames, passwords
3	February 7, 2017	August–December, 2106	InterContinental Hotels Group (IHG), parent company, owner of many properties	12 properties were affected including Crowne Plaza, Holiday Inn, Candlewood Suites, and more	Malware discovered on servers that processed payments at on-site hotel restaurants and bars; credit cards used at front desks were not compromised but cards used in restaurants and bars had information stolen, including cardholder names, card numbers, expiration dates, and internal verification codes.
4	February 17, 2017	Between October 25, 2016–January 29, 2017	Arby's	One third of 1,000 restaurants had malware; unsure how many compromised	Notified in mid January, but advised by FBI not to announce yet; malware placed on payment systems, not sure how many affected or what data stolen.
5	March 6, 2017	prior to March 6	River City Media Spammers	1.4 billion accounts, later revised to 393 million	"SpammerGate," a group of spammers, had their private data released into cyberspace after problem configuring their backups; Hipchat logs, domain registration records, accounting details, infrastructure planning, production notes, scripts, business affiliations, and more; Biggest discovery was a database of 1.4 billion email accounts, IP addresses, full names, and some physical addresses. The good news is the information was discovered by "good guys" - Chris Vickery, a security researcher for MacKeeper, who reported it to proper authorities. Thanks to aliases and affiliate programs, groups like River City Media are difficult to completely wipe out.
6	March 7, 2017	discovered January 2017, possibly since mid 2016	Verifone	unknown	Verifone says breach was only in the corporate network and didn't affect payment services network; claims misuse of info is limited; sources say a Russian hacking group is responsible
7	March 15, 2017	March 2017	Dun & Bradstreet	33 million	Email addresses, phone numbers, product codes, IP addresses
8	March 20, 2017	2014–2017	UNC Healthcare	1,300	Full names, addresses, races, ethnicities, Social Security numbers, variety of health-related information

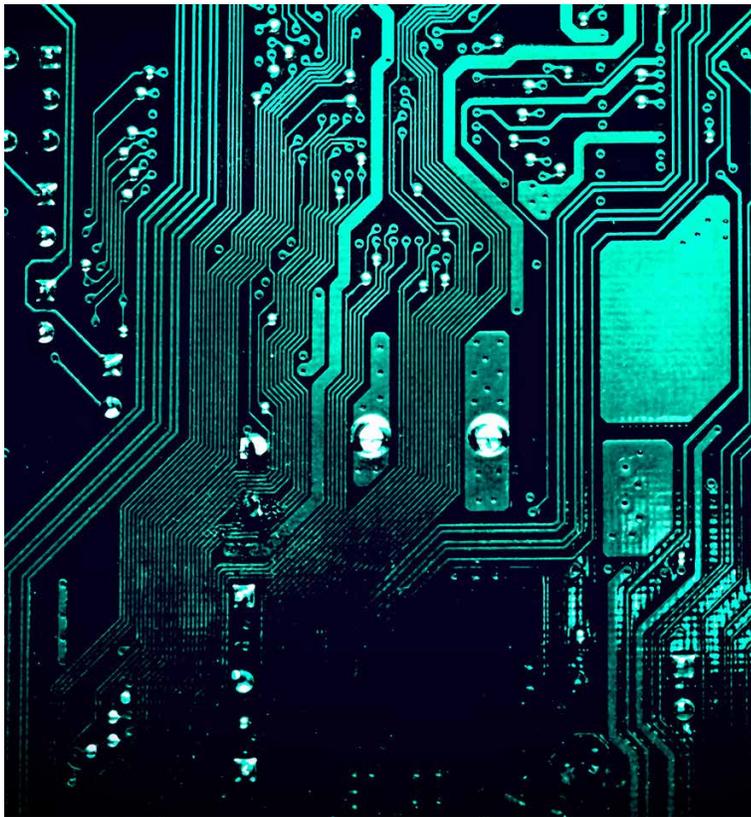
► Timeline of Significant Data Breaches

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
9	March 21, 2017	Month/years before March 14, 2017	America's Joblink	4.8 million	Full names, birth dates, and Social Security numbers
10	April 6, 2017	March 2017	FAFSA: IRS Data Retrieval Tool	100,000	Personal info possibly used to steal other info; 8,000 fraudulent returns filed costing \$32 million, 52,000 returns caught by filters, 14,000 illegal refunds stopped
11	April 19, 2017	August–March 2017	Intercontinental Hotels Group (IHG) Update	Update: reach of breach expanded from 12 properties to 1200	States malware in all hotel locations removed by end of March
12	April 25, 2017	March 24, 2017 through April 18, 2017	Chipotle	customers	Payment card transactions
13	March 2, 2017	not revealed	Sabre Hospitality Solutions	not revealed	Owns 36,000 properties but how many affected not disclosed; hotel customer payment information was compromised
14	May 3, 2017	May 2017, discovered in 1 hour	Gmail	1 million Gmail users	Phishing scam seeking to gain access to accounts through 3rd-party apps
15	May 10, 2017	2014–2017	Bronx Lebanon Hospital Center	At least 7,000 patients in New York	A misconfigured Rsync backup server led to the compromise of names, home addresses, religious affiliations, addiction histories, mental health and medical diagnoses, HIV statuses, and sexual assault and domestic violence reports; upon discovery, the hospital and iHealth took immediate steps to protect the exposed data
16	May 12, 2017	prior to May 17	DocuSign	Customers and users of Docusign	Hackers breached one of their systems and stole emails, using them to send out Docusign-branded phishing emails with malware
17	June 14, 2017	Records going back to 2002	University of Oklahoma	29,000	Private student information, education information, Social Security numbers, financial aid information, and grades
18	June 15, 2017	prior to June 15	Washington State University	1,000,000 people	Data on a hard drive stored in a safe was accessible through a research project; stolen data included Social Security numbers and health history, among other personal details; the university offered a free year of credit monitoring
19	June 20, 2017	Exposed for 2 weeks in June	Deep Root Analytics	198 million citizens	Personal data stored on Amazon cloud server, names, dates of birth, home addresses, phone numbers, and voter registration details

► Timeline of Significant Data Breaches

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
20	June 27, 2017	2015, \$115 million settlement paid	Blue Cross / Blue Shield / Anthem	80 million	Personal information
21	July 10, 2017	March 13, 2017– March 15, 2017	California Association of Realtors subsidiary	customers using online payment system	Real Estate Business Services (REBS) was breached through its store.car.org online payment system when it became infected with malware; users who made payments on the site may have had personal information stolen, including user's name, address, credit card number, credit card expiration date, and credit card verification codes; they are now using PayPal.
22	July 13, 2017	Late June	Verizon	14 million subscribers	Log files generated when customers contacted the company by phone
23	August 30, 2017		Online Spambot	711 million records	Similar to River City Media Breach, a spambot had harvested some email addresses and passwords harvested for sending spam emails, but forgot to secure the server the data was kept on; currently not known how many people accessed and are using the information for their own nefarious purposes
24	September 7, 2017	Mid May till discovered July 29, 2017	Equifax	143 million	Social Security numbers and driver's license numbers
25	September 21, 2017	2016 & 2017	US Securities and Exchange Comm (SEC)		2016 & 2017, discovered possible illegal trade gains due to breach; believed no personally identifiable information stolen
26	September 25, 2017	Discovered March 2017	Deloitte	unknown	Lacking two-factor authentication, hackers believed to gain access to all areas of the email system; Deloitte claims only a small number of clients affected
27	September 26, 2017	September 2017	Sonic	Possibly 5 million	Millions of stolen credit and debit card numbers discovered in fire sales on the Dark Web
28	September 28, 2017	September 2017	Whole Foods Market	unknown	Breach in payment systems affecting shoppers at Whole Foods taprooms and full table-service restaurants
29	October 9, 2017	2013	Yahoo!	Every Yahoo! Account, over 3 billion accounts	Account info across Yahoo! email, Tumblr, Fantasy, and Flickr accounts
30	October 12, 2017	Between March 18, 2017 and July 2, 2017	Hyatt Hotels	41 properties in 11 countries, including 5 in US territories	Unauthorized access to its payment card information for debit and credit cards that were swiped at the front desks of some of its properties resulted in stolen card numbers, expiration dates, internal verification codes, and cardholder names

	Date Announced	Date Occurred	Company	# of Users Affected	Data Affected
31	November 21, 2017	Late 2016	Uber	57 million Uber users & drivers	Names, email addresses, and phone numbers of Uber users worldwide, discovered after it was revealed Uber paid \$199k to cover up the hack
32	December 10, 2017	Unspecified	eBay	unknown	Personal information, including usernames, first and last names, and purchase history; also made available due to an improper feed signal with Google's Shopping platform; additional very personal information of HIV home test kits, pregnancy test, and drug testing kits was revealed
33	December 16, 2017	Unspecified	Alteryx	120,000 million American households	Personal information purchase form Experian, data was housed in AWS cloud storage bucket unprotected
Source: https://www.identityforce.com/blog/2017-data-breaches Source: https://www.identityforce.com/blog/2018-data-breaches					



226 Airport Parkway, Suite 350 • San Jose, CA 95110

Email: info@virsec.com • Phone: (877) 213-3558 • Web: www.virsec.com • Twitter: [virsecsystems](https://twitter.com/virsecsystems)