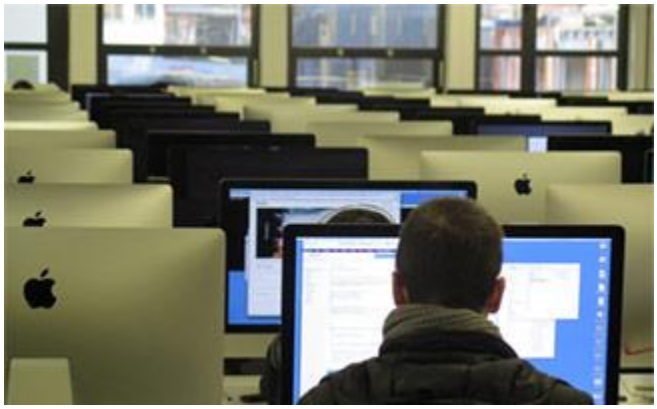
The Worst Data Breaches of the Last 10 Years

Posted by: Brianna Jensen, ASecurelife.com

September 18, 2017



http://www.asecurelife.com/the-worst-data-breaches-of-the-last-10-years/

Contents

Intro

Have you noticed more and more headlines about data breaches lately? You aren't imagining it—they've been on the rise in recent years. In fact, there was a **40% increase in data breaches** between 2015 and 2016. The numbers aren't all in on 2017 yet, but the trend seems to be continuing—Equifax, Instagram, and HBO are just three high-profile companies that have been breached this year.

We dug into the data from previous years to find some of the biggest and most high-profile data breaches of the last ten years. Many of these data breaches targeted social media sites, government institutions, medical organizations, and retailers, so **there's a good chance at least one of them affected you.**

Data breach highlights

Biggest

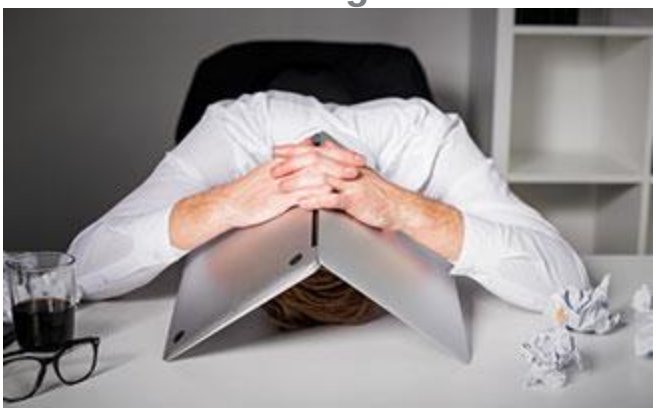
The **biggest data breach on record is probably River City Media** (a company known primarily for sending spammy emails)—it involved **a whopping 1.37 billion records**, exceeding even the 1 billion records breached in the Yahoo hack.

- In case you're having trouble wrapping your head around a number as colossal as 1.37 billion—that equates to almost one record for every single person in China.
- It's also fairly close to **the number of chicken wings Americans will eat on Super Bowl Sunday.**

Most serious

The recent Equifax data breach may be one of the **most serious data breaches** to date. Hackers got ahold of birthdates**, names, Social Security numbers, driver's** licence **numbers, addresses, and credit card numbers.** Current estimates suggest that this hack has affected 143 million Americans—nearly half of the population. The combination of banking information and personal identifying data makes this breach a treasure trove for identity thieves. If you're one of the millions whose information was stolen, it might be time to look into identity theft protection. (Just know that signing up through Equifax means you may be waiving your right to participate in a class action lawsuit later.)

Most embarrassing



One of the **most embarrassing data breaches** is one we already mentioned: River City Media. This record-breaking data breach was not the work of hackers—it was **an accident**. Backup databases that should have been secured were simply left available online. Oops.

Data breach timeline

2017

2017 isn't over yet, but SpaceX has successfully launched and recovered rockets, people in Japan have stood in lines spanning city blocks to get a chance at purchasing the Nintendo Switch, and people in the US drove for hours to watch the moon go in front of the sun for a few minutes.

We've also seen some significant data breaches. A few already stand out: Equifax, HBO, Instagram, and River City Media.

Equifax

Details are still emerging, but this looks to be **one of the most sensitive and serious data breaches** of the year. The hackers who hit the credit-reporting agency got Social Security numbers, banking information, and tons of other personal details.

- **Breach made public:** September 7, 2017
- **Number of records breached:** 143 million
- **Type of records accessed:** Social Security numbers, names, addresses, credit card numbers, and driver's license numbers.
- **Type of breach:** Hack
- **Company location:** Atlanta, Georgia

(Source)

HBO

The popular network is home to dragons approximately the size of aircraft carriers, but even impressive imaginary dragons couldn't protect the network

from real-world threats like hackers. So far the hack **doesn't seem to be quite as dire as the Sony hack** a few years earlier, but details are still emerging.

- **Breach made public:** July 31, 2017
- **Number of records breached:** Unknown
- **Type of records accessed:** Upcoming episodes of TV shows, executive emails, scripts for Game of Thrones
- **Type of breach:** Hack
- **Company location:** New York, New York

(Source)

Instagram

A bug left Instagram vulnerable to a hack that**targeted celebrities**—but it also affected normal users. The good news is that if you were one of those six million users, you now have something in common with Beyoncé, Leonardo DiCaprio, and Zac Efron. Congrats!

- **Breach made public:** August 30, 2017
- **Number of records breached:** Data for over 6 million users
- **Type of records accessed:** Email addresses and phone numbers
- **Type of breach:** Hack
- **Company location:** Meno Park, California

(Source)

River City Media

This may be the largest data breach we've ever seen. And it was an **accident.** We aren't particularly rooting for a company known for sending annoying emails that clog up your inbox, but the scale of the breach is a bit alarming.

- Breach made public: March 8, 2017
- Number of records breached: 1.37 billion
- Type of records accessed: Email addresses and information connected with those addresses (names of users, IP addresses, physical addresses of users)
- Type of breach: Unintentional—backup databases were left accessible online
- Company location: Portland, Oregon

(Source)

2016

Google finally entered the smartphone market in 2016 with the Google Pixel. And drones got much more portable and consumer friendly when DJI released the foldable Mavic Pro with a 4K stabilized camera.

Sports were also a big deal in 2016. Many of us took a break from the incessant election coverage to watch the feats of athletes in the Rio Summer Olympics. Later that year the Chicago Cubs defied the odds to finally win the World Series for the **first time in over 100 years.** While sports may have been a nice distraction, the presidential election certainly dominated during 2016. And the year's most notable data breach also revolved around the election.

Democratic National Committee

Coverage of the 2016 election was exhaustive, so we're not going to say much here.

- **Breach made public:** June 14, 2016
- **Number of records breached:** Unknown
- **Type of records accessed:** Information about Democratic candidates (including presidential candidate Hillary Clinton), opposition research about presidential candidate Donald Trump
- **Type of breach:** Hack
- **Company location:** Washington, DC

(Source)

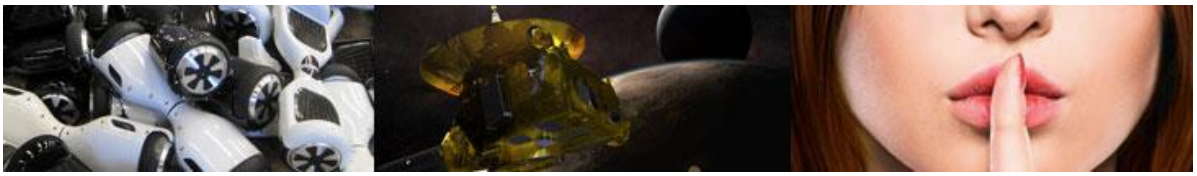
FriendFinder

While the DNC hack was a big deal, it wasn't the only big data breach in 2016. The hack of FriendFinder involved 412 million records and information that went back 20 years. While finding friends sounds benign, the **FriendFinder network is also home to adult content** on Adult FriendFinder, Penthouse, Cams.com, and other similar websites with more sensitive—and potentially embarrassing—content.

- **Breach made public:** November 16, 2016
- **Number of records breached:** 412 million
- **Type of records accessed:** 20 years of account information such as passwords, emails, usernames, and dates of website visits
- **Type of breach:** Hack
- **Company location:** Sunnyvale, California

(Source), (Source)

2015



In 2015 the world fell in love with exploding hoverboards and Pluto's icy heart. But 2015 was also a big year for data breaches—and love may have gotten some people in trouble.

Ashley Madison

Data breaches can cause a lot of damage—but to be honest it was a bit difficult to feel sorry for those affected in this case since Ashley Madison **caters to people looking online for extramarital affairs.**

- **Breach made public:** July 19, 2015
- **Number of records breached:** 37 million
- **Type of records accessed:** Account details and login information for users, credit card details, addresses, and phone numbers
- **Type of breach:** Hack
- **Company location:** Canada

(Source), (Source)

Anthem

While this data breach was perhaps less flashy than the Ashley Madison breach, it was just as damaging. The hackers who targeted this insurance company got a hold of **sensitive data that could be used for identity theft**—including things like Social Security numbers and street addresses.

- **Breach made public:** February 5, 2015
- **Number of records breached:** 80 million
- **Type of records accessed:** Social Security numbers, email addresses, names, birthdays, street addresses, and income information
- **Type of breach:** Hack
- **Company location:** Indianapolis, Indiana

(Source)

Office of Personnel Management

If you're a **government employee with a security clearance**, it seems fair to expect that when you keep government information secret, the government will return the favor. Unfortunately, the OPM hack meant these employees had their own information exposed—including, in some cases, fingerprints. The breach affected at least 18 million individuals.

- **Breach made public:** June 4, 2015
- **Number of records breached:** 21.5 million
- **Type of records accessed:** Social Security numbers, fingerprints, information about employee job assignments and training
- **Type of breach:** Hack
- **Company location:** Washington, DC

(Source)

2014

Apple made its way into the wearable market with the Apple Watch in 2014, while Amazon took our Internet of Things obsession to the next level with Amazon Alexa.

People also spent time watching the Sochi Olympics and reading the fascinating emails about the inner workings of Sony.

Sony Pictures Entertainment

This breach was a lot smaller than companies that had millions of records stolen, but it had a huge impact because it exposed the messy inner workings of Sony Pictures Entertainment. The hack highlighted a lot of embarrassing issues within the company, but there was a bright spot in the bureaucratic murk: we found out that Channing Tatum's emails are hilarious.

- **Breach made public:** November 24, 2014
- **Number of records breached:** 47,000
- **Type of records accessed:** Internal emails, private messages, unreleased films, financial data, and contact information for actors
- **Type of breach:** Hack
- **Company location:** New York, New York

(Source), (Source)

JPMorgan Chase

This hack affected 76 million households, which made it **even worse than previous hacks that hit retailers like Target and Home Depot.** It was also more damaging because banks have more sensitive information about customers than retailers do.

- **Breach made public:** August 28, 2014
- **Number of records breached:** 76 million
- **Type of records accessed:** Bank account information, names, addresses, and phone numbers
- **Type of breach:** Hack
- **Company location:** New York, New York

(Source), (Source)

2013



In 2013 Sony released the long-awaited PlayStation 4, Edward Snowden became a household name, and Fitbit released its first fitness tracker that could be worn on the wrist.

While Snowden's leaks were monumental, there were quite a few other significant data breaches during 2013—and the **biggest one wasn't even made public until 2016.**

Yahoo

This colossal breach occurred in 2013 but **wasn't discovered until the end of 2016.** And this wasn't the only huge Yahoo data breach—another **500 million records** were breached in 2014.

- **Breach made public:** December 14, 2016
- **Number of records breached:** 1 billion
- **Type of records accessed:** Email addresses, birthdays, and answers to security questions, codes that allow hackers to access accounts without a password
- **Type of breach:** Hack
- **Company location:** Sunnyvale, California

(Source), (Source)

Target

This breach hit **just in time for the holiday shopping season.** Ouch. Even many years later, this is still one of the biggest hacks people think of when you mention data breaches.

- **Breach made public:** December 13, 2013
- **Number of records breached:** 40 million
- **Type of records accessed:** Credit and debit account information including customer name, card number, security code, and expiration date
- **Type of breach:** Hack
- **Company location:** Minneapolis, Minnesota

(Source), (Source)

2012

The Mayan calendar ended in 2012, but the world is still here. Those who weren't anticipating the end of days spent 2012 watching the London Olympics, swiping right (or left) with the new, addictive dating app Tinder, and obsessing over the K-pop song "Gangnam Style."

2012's data breaches were a little less glamorous and exciting than the other things going on in 2012, but if you used **LinkedIn or Dropbox**, these data breaches may have caught your attention.

LinkedIn

If you were using LinkedIn in 2012, you probably had to **reset your password.** The professional networking site was the victim of a hack that breached millions or records. LinkedIn responded to the hack the day after it happened and enforced a mandatory password reset for the accounts that they knew were affected.

- **Breach made public:** June 6, 2012
- **Number of records breached:** 167 million
- **Type of records accessed:** Encrypted passwords and email addresses
- **Type of breach:** Hack
- **Company location:** Mountain View, California

(Source), (Source)

Dropbox

One of the accounts accessed in this hack was an employee account. This account **contained a document with user email addresses.** Oops.

- **Breach made public:** July 17, 2012
- **Number of records breached:** 68 million
- **Type of records accessed:** Email addresses and passwords
- **Type of breach:** Unknown, but likely hackers
- **Company location:** San Francisco, California

(Source)

2011

Artificial intelligence conquered humans in 2011—on the long-running game show Jeopardy! Many of the humans who weren't losing trivia games to computers used their time counting down the days until a British prince married a woman with infuriatingly flawless hair.

There weren't a lot of notable data breaches in 2011, but if you're a gamer you might remember the **Sony PlayStation hack.**

While Snowden's leaks were monumental, there were quite a few other significant data breaches during 2013—and the biggest one wasn't even made public until 2016.

Sony PlayStation Network

Sony's data breach problems started before the high-profile 2014 hack. The **hack in 2011 was also incredibly damaging** and resulted in quite a few angry customers.

- **Breach made public:** April 27, 20011
- **Number of records breached:** 101.6 million
- **Type of records accessed:** 12 million unencrypted credit card numbers, names, physical addresses, birthdays, passwords, answers to security questions, and email addresses
- **Type of breach:** Hack
- **Company location:** New York, New York

(Source)

2010

2010 was the year Apple released the first iPad, Toy Story 3 won at the box office, and a new species of toad was discovered in Colombia. Exciting stuff.

There weren't a lot of notable data breaches in 2010, but your true best friend, **Netflix, did run into a few problems that year.**

Netflix

In an effort to improve its movie recommendation system, Netflix held a contest that provided participants with data sets including subscriber movie ratings and preferences. Netflix did not consider this a data breach. However, consumers weren't so sure. Plaintiffs **filed a class action lawsuit** citing the fact that many researchers were able to use the anonymized data set to identify individual subscribers.

- **Breach made public:** January 1, 2010
- **Number of records breached:** 100 million records tying back to 480,000 subscribers
- **Type of records accessed:** Anonymized subscriber information about movie preferences
- **Type of breach:** Voluntary—Netflix does not consider it a breach.
- **Company location:** Los Gatos, California

(Source)

2009

2009 was year of big discoveries—scientists found water on the moon, and Usher introduced the world to your little sister's worst obsession—Justin Bieber.

On the tech front, Motorola's Droid finally gave the iPhone some real competition, and the Canon 1D Mark IV was at the top of the pack with 16 megapixels and the ability to shoot HD video.

While 2009 was a pretty good year for companies making smartphones, one of the **major carriers had a rough patch** thanks to some greedy employees in England.

T-Mobile

Data breaches aren't always caused by sophisticated hackers. Sometimes one or two bad employees with access to sensitive information can do just as much damage as a larger organization.

- **Breach made public:** November 2009
- **Number of records breached:** Exact number is unknown, but it was in the millions and included data from over 500,000 customers

- **Type of records accessed:** names, addresses, phone numbers, and contract renewal dates
- **Type of breach:** Employees stole the data and sold it to competitors
- **Company location:** England

  (Source), (Source)

2008

2008 was the year **Barack Obama was elected as president of the United States and the Hadron Collider was switched on for the first time.** It was also a pretty rough year in the US and across the world financially speaking. And while the financial downturn hurt individuals, banks and other large companies also sustained significant losses thanks to huge data breaches.

Heartland Payment Systems

The theft occurred from late 2006 to 2008 and resulted in **significant financial losses.**

- **Breach made public:** January 20, 2009
- **Number of records breached:** Over 130 million
- **Type of records accessed:** Credit and debit card numbers
- **Type of breach:** Hack
- **Company location:** Princeton, New Jersey

  (Source), (Source)

American Business Hack

This data breach **affected multiple companies, including Nasdaq and 7-Eleven.** Like the Heartland data breach, this one spanned multiple years—data was actually being stolen from 2005 to 2012. We placed it in 2008 because a large portion of the records were stolen between 2008 and 2009 during the economic downturn.

- **Breach took place:** From 2005 to 2012
- **Number of records breached:** Unknown—at least 160 million credit and debit card numbers. It resulted in at least $300 million in losses to companies and individuals.
- **Type of records accessed:** Credit and debit card numbers, usernames, passwords
- **Type of breach:** Hack

  (Source)

Throwback hack: 1984

Data breaches aren't exclusive to this century. If you were alive in 1984, you may remember the first Apple Macintosh or Michael Jordan being drafted by the Chicago Bulls at the very beginning of his career.

1984 was also the year when **a stolen password led to one of the first data breaches on record.**

Sears/TRW Information Systems

Looking back, it's hard to imagine that **one password could lead to 90 million records.** Yikes.

- **Breach made public:** June 1984
- **Number of records breached:** 90 million
- **Type of records accessed:** A password that permitted access to names, Social Security numbers, birthdates, and addresses
- **Type of breach:** Stolen password
- **Company location:** Chicago, Illinois

(Source)

Should you be worried about data breaches?

If you aren't running a major corporation, you probably haven't suffered huge losses at the hands of hackers, but data breaches can still affect you—particularly if one of the companies targeted in an attack has your personal information. That **information could easily end up in the hands of identity thieves**, which could cause real problems for you down the road.

If you're worried about your information being exposed during a data breach, we suggest investing in credit monitoring and identity theft protection. We also recommend creating strong passwords, keeping your information close to the vest, and giving it out only when absolutely necessary.