Reference <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

**The 15 biggest data breaches of the 21st century**

**Data breaches affecting millions of users are far too common. Here are some of the biggest, baddest breaches in recent memory.**

* By [Michael Hill](https://www.csoonline.com/author/Michael-Hill/) and [Dan Swinhoe](https://www.csoonline.com/author/Dan-Swinhoe/)

           CSO |   Jul 16, 2021 2:00 am PDT



In today’s data-driven world, data breaches can affect hundreds  of millions or even billions of people at a time. Digital transformation has increased the supply of data moving, and data breaches have scaled  up with it as attackers exploit the data-dependencies of daily life. How large cyberattacks of the future might become remains speculation, but  as this list of the biggest data breaches of the 21st Century indicates, they have already reached enormous magnitudes.

[ Learn the [The 5 types of cyberattack you're most likely to face](https://www.csoonline.com/article/2616316/the-5-types-of-cyber-attack-youre-most-likely-to-face.html). | Get the latest from CSO by [signing up for our newsletters](http://www.csoonline.com/newsletters/signup.html). ]

For transparency, this list has been calculated by the number of users impacted, records exposed, or accounts affected. We have also  made a distinction between incidents where data was actively stolen or  reposted maliciously and those where an organization has inadvertently  left data unprotected and exposed, but there has been no significant  evidence of misuse. The latter have purposefully not been included in  the list.

So, here it is – an up-to-date list of the 15 biggest  data breaches in recent history, including details of those affected,  who was responsible, and how the companies responded (as of July 2021).

**1. Yahoo**

**Date:** August 2013  
**Impact:** 3 billion accounts



Securing the number one spot – almost seven years after the [initial breach](https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html) and four since the true number of records exposed was revealed – is the attack on Yahoo. The company first publicly announced the incident –  which it said took place in 2013 – in December 2016. At the time, it was in the process of being acquired by Verizon and estimated that account  information of more than a billion of its customers had been accessed by a hacking group. Less than a year later, Yahoo announced that the  actual figure of user accounts exposed was 3 billion. Yahoo stated that  the revised estimate did not represent a new “security issue” and that  it was sending emails to all the “additional affected user accounts.”

Despite the attack, the deal with Verizon was completed, albeit at a reduced  price. Verizon’s CISO Chandra McMahon said at the time: “Verizon is  committed to the highest standards of accountability and transparency,  and we proactively work to ensure the safety and security of our users  and networks in an evolving landscape of online threats. Our investment  in Yahoo is allowing that team to continue to take significant steps to  enhance their security, as well as benefit from Verizon’s experience and resources.” After investigation, it was discovered that, while the  attackers accessed account information such as security questions and  answers, plaintext passwords, payment card and bank data were not  stolen.

**2. Alibaba**

**Date:** November 2019  
**Impact:** 1.1 billion pieces of user data

Over an eight-month period, a developer working for an affiliate  marketer scraped customer data, including usernames and mobile numbers,  from the Alibaba Chinese shopping website, Taobao, using crawler  software that he created. It appears the developer and his employer were collecting the information for their own use and did not sell it on the black market, although both were sentenced to three years in prison.

**3. LinkedIn**

**Date:** June 2021  
**Impact:**700 million users

Professional networking giant LinkedIn saw data associated with 700 million of its  users posted on a dark web forum in June 2021, impacting more than 90%  of its user base. A hacker going by the moniker of “God User” used data  scraping techniques by exploiting the site’s (and others’) API before  dumping a first information data set of around 500 million customers.  They then followed up with a boast that they were selling the full 700  million customer database. While LinkedIn argued that as no sensitive,  private personal data was exposed, the incident was a violation of its  terms of service rather than a data breach, a scraped data sample posted by God User contained information including email addresses, phone  numbers, geolocation records, genders and other social media details,  which would give malicious actors plenty of data to craft convincing,  follow-on social engineering attacks in the wake of the leak, as [warned by the UK’s NCSC](https://www.ncsc.gov.uk/report/weekly-threat-report-2nd-july-2021#section_2).

**4. Sina Weibo**

**Date:** March 2020  
**Impact:** 538 million accounts

Cloud perceptions  study reveals fascinating insights around redundancy, data movement,  workloads, and cloud transformation.  Discover self-evaluation and  action plans for immediate results.

With over 600 million users, Sina Weibo is one of  China’s largest social media platforms. In March 2020, the company  announced that an attacker obtained part of its database, impacting 538  million Weibo users and their personal details including real names,  site usernames, gender, location, and phone numbers. The attacker is  reported to have then sold the database on the dark web for $250.

China’s Ministry of Industry and Information Technology (MIIT) ordered Weibo to enhance its data security measures to better protect personal  information and to notify users and authorities when data security  incidents occur. In a [statement](https://passport.weibo.com/visitor/visitor?entry=miniblog&a=enter&url=https%3A%2F%2Fweibo.com%2F2735327001%2FIzCMJioqC%3Ffrom%3Dpage_1006062735327001_profile%26wvr%3D6%26mod%3Dweibotime%26type%3Dcomment&domain=.weibo.com&sudaref=https%3A%2F%2Fwww.campaignasia.com%2F&ua=php-sso_sdk_client-0.6.36&_rand=1624874184.8443), Sina Weibo argued that an attacker had gathered publicly posted  information by using a service meant to help users locate the Weibo  accounts of friends by inputting their phone numbers and that no  passwords were affected. However, it admitted that the exposed data  could be used to associate accounts to passwords if passwords are reused on other accounts. The company said it strengthened its security  strategy and reported the details to the appropriate authority.

**5. Facebook**

**Date:** April 2019  
**Impact:** 533 million users

In April 2019, [it was revealed](https://www.upguard.com/breaches/facebook-user-data-leak) that two datasets from Facebook apps had been exposed to the public  internet. The information related to more than 530 million Facebook  users and included phone numbers, account names, and Facebook IDs.  However, two years later (April 2021) the data was posted for free,  indicating new and real criminal intent surrounding the data. In fact,  given the sheer number of phone numbers impacted and readily available  on the dark web as a result of the incident, security researcher Troy  Hunt added functionality to his HaveIBeenPwned (HIBP) breached  credential checking site that would allow users to verify if their phone numbers had been included in the exposed dataset.

“I’d never planned to make phone numbers searchable,” [Hunt wrote in blog post](https://www.troyhunt.com/the-facebook-phone-numbers-are-now-searchable-in-have-i-been-pwned/). “My position on this was that it didn’t make sense for a bunch of  reasons. The Facebook data changed all that. There’s over 500 million  phone numbers but only a few million email addresses so >99% of  people were getting a miss when they should have gotten a hit.”

**6. Marriott International (Starwood)**

**Date:**September 2018  
**Impact:** 500 million customers

Hotel Marriot International announced the [exposure of sensitive details](https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html) belonging to half a million Starwood guests following an attack on its  systems in September 2018. In a statement published in November the same year, the hotel giant said: “On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading  security experts to help determine what occurred.”

Marriott  learned during the investigation that there had been unauthorized access to the Starwood network since 2014. “Marriott recently discovered that  an unauthorized party had copied and encrypted information and took  steps towards removing it. On November 19, 2018, Marriott was able to  decrypt the information and determined that the contents were from the  Starwood guest reservation database,” the statement added.

The  data copied included guests’ names, mailing addresses, phone numbers,  email addresses, passport numbers, Starwood Preferred Guest account  information, dates of birth, gender, arrival and departure information,  reservation dates, and communication preferences. For some, the  information also included payment card numbers and expiration dates,  though these were apparently encrypted.

Marriot carried out an  investigation assisted by security experts following the breach and  announced plans to phase out Starwood systems and accelerate security  enhancements to its network. The company was eventually [fined £18.4 m](https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/)illion (reduced from £99 million) by UK data governing body the Information  Commissioner's Office (ICO) in 2020 for failing to keep customers’  personal data secure. An article by [New York Times](https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html) attributed the attack to a Chinese intelligence group seeking to gather data on US citizens.

**7. Yahoo**

**Date:** 2014  
**Impact:** 500 million accounts

Making its second appearance in this list is Yahoo, which suffered an attack  in 2014 separate to the one in 2013 cited above. On this occasion,  state-sponsored actors stole data from 500 million accounts including  names, email addresses, phone numbers, hashed passwords, and dates of  birth. The company took initial remedial steps back in 2014, but it  wasn’t until 2016 that Yahoo went public with the details after a stolen database went on sale on the black market.

**8. Adult Friend Finder**

**Date:** October 2016  
**Impact:** 412.2 million accounts

The adult-oriented social networking service The FriendFinder Network had  20 years’ worth of user data across six databases stolen by  cyber-thieves in October 2016. Given the sensitive nature of the  services offered by the company – which include casual hookup and adult  content websites like Adult Friend Finder, Penthouse.com, and  Stripshow.com – the breach of data from more than 414 million accounts  including names, email addresses, and passwords had the potential to be  particularly damming for victims. What’s more, the vast majority of the  exposed passwords were hashed via the notoriously weak algorithm SHA-1,  with an estimated 99% of them cracked by the time LeakedSource.com  published its analysis of the data set on November 14, 2016.

**9. MySpace**

**Date:** 2013  
**Impact:** 360 million user accounts

Though it had long stopped being the powerhouse that it once was, social media site MySpace hit the headlines in 2016 after 360 million user accounts  were leaked onto both LeakedSource.com and put up for sale on dark web  market The Real Deal with an asking price of 6 bitcoin (around $3,000 at the time).

According to [the company](https://myspace.com/pages/blog), lost data included email addresses, passwords and usernames for “a  portion of accounts that were created prior to June 11, 2013, on the old Myspace platform. In order to protect our users, we have invalidated  all user passwords for the affected accounts created prior to June 11,  2013, on the old Myspace platform. These users returning to Myspace will be prompted to authenticate their account and to reset their password  by following instructions.”

It’s believed that the passwords were stored as SHA-1 hashes of the first 10 characters of the password converted to lowercase.

**10. NetEase**

**Date:** October 2015  
**Impact:** 235 million user accounts

NetEase, a provider of mailbox services through the likes of 163.com and  126.com, reportedly suffered a breach in October 2015 when email  addresses and plaintext passwords relating to 235 million accounts were  being sold by dark web marketplace vendor DoubleFlag. NetEase has  maintained that no data breach occurred and to this [day HIBP states](https://haveibeenpwned.com/PwnedWebsites#NetEase): “Whilst there is evidence that the data itself is legitimate (multiple  HIBP subscribers confirmed a password they use is in the data), due to  the difficulty of emphatically verifying the Chinese breach it has been  flagged as “unverified.”

**11. Court Ventures (Experian)**

**Date:** October 2013  
**Impact:** 200 million personal records

Experian subsidiary Court Ventures fell victim in 2013 when a Vietnamese man [tricked it](https://www.computerworld.com/article/2948295/vietnamese-man-gets-13-years-for-massive-id-theft-scheme.html)into giving him access to a database containing 200 million personal records by posing as a private investigator from Singapore. The details of Hieu Minh Ngo’s exploits only came to light following his arrest for selling personal information of US residents (including credit card numbers and Social Security numbers) to cybercriminals across the world, something  he had been doing since 2007. In March 2014, he pleaded guilty to  multiple charges including identity fraud in the US District Court for  the District of New Hampshire. The DoJ stated at the time that Ngo had  made a total of $2 million from selling personal data.

**12. LinkedIn**

**Date:** June 2012  
**Impact:** 165 million users

With its second appearance on this list is LinkedIn, this time in reference  to a breach it suffered in 2012 when it announced that 6.5 million  unassociated passwords (unsalted SHA-1 hashes) had been stolen by  attackers and posted onto a Russian hacker forum. However, it wasn’t  until 2016 that the full extent of the incident was revealed. The same  hacker selling MySpace’s data was found to be offering the email  addresses and passwords of around 165 million LinkedIn users for just 5  bitcoins (around $2,000 at the time). LinkedIn [acknowledged](https://blog.linkedin.com/2016/05/18/protecting-our-members) that it had been made aware of the breach, and said it had reset the passwords of affected accounts.

**13. Dubsmash**

**Date:** December 2018  
**Impact:** 162 million user accounts

In December 2018, New York-based video messaging service Dubsmash had 162  million email addresses, usernames, PBKDF2 password hashes, and other  personal data such as dates of birth stolen, all of which was then put  up for sale on the Dream Market dark web market the following December.  The information was being sold as part of a collected dump also  including the likes of MyFitnessPal (more on that below), MyHeritage (92 million), ShareThis, Armor Games, and dating app CoffeeMeetsBagel.

Dubsmash acknowledged the breach and sale of information had occurred and  provided advice around password changing. However, it failed to state  how the attackers got in or confirm how many users were affected.

**14. Adobe**

**Date:** October 2013  
**Impact:** 153 million user records

In early October 2013, [Adobe reported](https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/) that hackers had stolen almost three million encrypted customer credit  card records and login data for an undetermined number of user accounts. Days later, Adobe increased that estimate to include IDs and encrypted  passwords for 38 million “active users.” Security blogger Brian Krebs  then reported that a file posted just days earlier “appears to include  more than 150 million username and hashed password pairs taken from  Adobe.” Weeks of research showed that the hack had also exposed customer names, password, and debit and credit card information. An agreement in August 2015 called for Adobe to pay $1.1 million in legal fees and an  undisclosed amount to users to settle claims of violating the Customer  Records Act and unfair business practices. In November 2016, the amount  paid to customers was reported to be $1 million.

**15. My Fitness Pal**

**Date:** February 2018  
**Impact:** 150 million user accounts

In February 2018, diet and exercise app MyFitnessPal (owned by Under  Armour) exposed around 150 million unique email addresses, IP addresses  and login credentials such as usernames and passwords stored as SHA-1  and bcrypt hashes. The following year, the data appeared for sale on the dark web and more broadly. The company [acknowledged the breach](https://content.myfitnesspal.com/security-information/FAQ.html) and said it took action to notify users of the incident. “Once we  became aware, we quickly took steps to determine the nature and scope of the issue. We are working with leading data security firms to assist in our investigation. We have also notified and are coordinating with law  enforcement authorities,” it stated.