

? Join our Product Deep Dive Webinar with live Q&A! Register Now | Looking to streamline your TPRM? Join our Product Deep Dive Webinar with live Q&A! Register Now



Products Solutions Pricing Resources Customers Tour Login [Free trial](#) [Get a demo](#)

Blog Data Breaches Biggest Data Breaches in US History (Updated 2025)

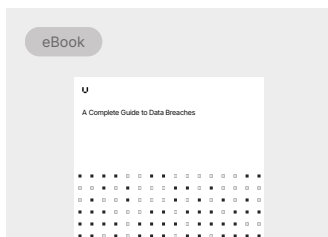
Biggest Data Breaches in US History (Updated 2025)

[Download the PDF guide](#) →

[Free trial](#)



Kyle Chin — Updated June 30, 2025



Free resource

A Complete Guide to Data Breaches

Learn how to avoid a costly data breach with a comprehensive prevention strategy.

Download now

Everyone is at risk of a [data breach](#) or [cyber attack](#), no matter how small or large a company is. Hackers and cybercriminals come up with new ways every day to steal sensitive information or personal data that they can potentially sell or [ransom for money](#).

According to a [report](#) published by the Identity Theft Resource Center (ITRC), a record number of 1862 data breaches occurred in 2021 in the US. This number broke the previous record of 1506 set in 2017 and represented a 68% increase compared to the 1108 breaches in 2020. Sectors like [healthcare](#), [finance](#), business, and retail are the most commonly attacked, impacting millions of Americans every year.

Many [cybersecurity](#) experts believe that this number will continue to increase in 2023 and beyond. To help you understand the [scope and extent of data breaches](#) today, here are the largest data breaches in US history.

Is Your Business at Risk of a [Data Breach](#)? [Find out now →](#)

26 Biggest Data Breaches in US History

When a data breach occurs, [sensitive data](#) can be stolen and sold on the [dark web](#) or to third parties. Here are some of the biggest data breaches in history that led to the exposure of millions of user records.



1. Yahoo!

Date: 2013-2016

Impact: Over 3 billion user accounts exposed

The data breach of [Yahoo](#) is one of the worst and most infamous cases of a known cyberattack and currently holds the record for the most people affected. The first attack occurred in 2013, and many more would continue over the next three years.

A team of Russian hackers targeteded Yahoo's database using backdoors, stolen backups, and access cookies to steal records from all user accounts, which included [personally identifiable information \(PII\)](#) like:

Security First Innovations, LLC, Exhibit 2034

Page 2034 - 2

- Names
- Email addresses
- Phone numbers
- Birth dates
- Passwords
- Calendars
- Security questions

Initially, Yahoo reported stolen data from about 1 billion accounts. However, after [Verizon](#) bought out Yahoo in 2017, they reported that the final number of records totaled about 3 billion accounts affected. Not only was Yahoo slow to react, but the company also failed to disclose a 2014 incident to users, which resulted in a \$35 million fine and, in total, 41 class-action lawsuits.

[Learn about the top Vendor Risk Management solution options on the market >](#)



2. Microsoft

Date: January 2021

Impact: 30,000 US companies (60,000 companies worldwide)

[In one of the largest cyberattacks](#) in US history, over 30,000 US businesses were affected by a sweeping attack on the Microsoft Exchange email servers, one of the largest email servers in the world. The hackers were able to [exploit](#) four different [zero-day vulnerabilities](#) that allowed them to gain unauthorized access to emails from small businesses to local governments.

For three months, hackers took advantage of a few coding errors to allow them to take control of vulnerable systems. They only needed two conditions to break into each individual company's email servers:

1. Connection to the internet
2. On-premises, locally managed systems

Once they were in, they could request access to data, deploy [malware](#), use backdoors to gain access to other systems, and ultimately take over the servers. Since the requests looked like they came from the Exchange servers themselves, many people assumed it was legitimate and approved.

[Learn how to respond to the Fortigate SSL VPN vulnerability >](#)

Though [Microsoft](#) was able to patch the [vulnerabilities](#), if the owners of the individual servers didn't update their systems, attackers would be able to exploit the system flaw again. Because the systems weren't on the cloud, Microsoft couldn't push a patch to fix the issues immediately.

In July 2021, the [Biden administration](#), along with the FBI, accused China of the data breach. Microsoft followed suit and named a Chinese state-sponsored hacker group, Hafnium, as the culprit behind the attack.



3. Real Estate Wealth Network

Date: December 2023

Impact: 1.5 billion records leaked

In one of the largest leaks in US history, a New York-based online real estate education platform, [Real Estate Wealth Network](#), exposed more than 1.5 billion records in their database to the public. The database contained nearly 1.16 TB of data, which was exposed for an unknown period due to having non-password-protected folders and system access. Among the exposed data included:

- Names, addresses, phone numbers
- Property history
- Court judgements
- Buyer and seller information
- Mortgage information
- Homeowner's association (HOA) liens
- Obituary information
- Bankruptcy information
- Tax IDs and other tax information

More notably, information such as property ownership data could be found on major celebrities, which included individuals like Kylie Jenner, Britney Spears, Floyd Mayweather, Nancy Pelosi, and more. With this information, cybercriminals could easily carry out social engineering attacks, commit financial fraud, or execute other cyber attacks.

Representatives from Real Estate Wealth Network confirmed they owned the database, but it is currently unclear if they are undergoing investigation or legal action.



The First American Corporation

4. First American Financial Corp.

Date: May 2019

Impact: 885 million file records leaked

In 2019, [First American Financial Corp.](#) suffered a major [data leak](#) due to poor [data security](#) measures and faulty website design. Although this incident was labeled a data leak instead of a breach (no hacking involved), it shows just how easily sensitive information can fall into the wrong hands.

Due to a website design error called Insecure Direct Object Reference

Security First Innovations, LLC, Exhibit 2034

Page 2034 - 4

IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Due to a website design error called **insecure Direct Object Reference (IDOR)**, access to private information was allowed without needing verification or authentication procedures. As a result, anyone with a link to the documents could view them freely. On top of that, because First American logged their records in sequential order, users could simply change the number in the URL to view other customer records.

Approximately 885 million files were exposed, including:

- Bank account numbers
- Bank statements
- Mortgage payments documents
- Wire transfer receipts with social security numbers
- Drivers' licenses

Fortunately, no data was compromised or exploited. Because First American violated cybersecurity laws due to ignoring red flags in 2018 and other administrative errors, they were ultimately fined roughly \$500,000 by the Securities and Exchange Commission (SEC).

[Learn how to respond to the MOVEit Transfer zero-day >](#)



5. Facebook

Date: April 2021

Impact: 530 million users exposed

Although one of the world's largest companies, **Facebook** is no stranger to data leaks and controversy. The social media giant has constantly dealt with security breaches of user data since the company went public in 2012.

The company's massive data breach in April 2021 was one of its largest, leaking names, phone numbers, account names, and passwords of over 530 million people to the public. Facebook identified the problem in the platform's tool to sync contacts, citing hackers exploiting a vulnerability to scrape user profiles for customer data.

Though Facebook maintained that no data had been compromised or misused, it's impossible to verify since the information was public for a short period. Hackers or scammers can easily take advantage of unsuspecting users with just their names, phone numbers, and emails.

Since 2013, Facebook has faced multiple major data breaches, including:

- In March 2019, information leaked that Facebook employees had access to over 600 million user accounts. Account IDs and passwords for both Facebook and Instagram were stored in plaintext files. Although Facebook claims no sensitive information was exposed, it was one more incident among many security issues.
- In April 2019, the Cyber Risk team at UpGuard [discovered 540 million unsecured Facebook user data records on public Amazon S3 cloud servers](#). Third-party app developer and Mexican media company Cultura Colectiva failed to password-protect their entire dataset, leaving the information open for anyone to access and download.
- Although Facebook was not directly responsible for this incident, it

brought scrutiny to how the social network managed third-party access to its database. Following a long history of data leaks, Facebook finally increased restrictions on third-party developers.

- Just a few months later, more exposed records were found on a foreign server on the dark web. Further investigation found that a hacker group in Vietnam may have abused Facebook's API and scraped the site for user IDs, names, and phone numbers. Over 300 million users were affected.

Facebook / Cambridge Analytica

Date: April 2018

Impact: 50-90 million users exposed

In 2018, a British consulting firm, Cambridge Analytica, stole and sold data from 50-90 million user accounts on Facebook in one of the most high-profile cases in recent memory. Cambridge Analytica security researcher Aleksandr Kogan accessed this data through a loophole from a third-party quiz app. This loophole in Facebook's API (application programming interface) allowed Kogan to compile data from anyone who downloaded the app and their entire friend network.

Despite going against the terms and conditions of Facebook, Cambridge Analytica continued to sell the data illegally because there was no rule enforcement. Reports show that Facebook was aware of the issue as early as 2015 but did not take action until Christopher Wylie, a Cambridge Analytica employee, blew the whistle.

Things finally came to a head when the Federal Trade Commission (FTC) announced a historic \$5 billion fine for Facebook's continuous violation of data security and poor data protection practices. The FTC also mandated a complete restructuring from the top down to increase oversight of privacy compliance. Furthermore, the FTC filed a lawsuit against Cambridge Analytica, forcing CEO Alexander Nix to resign.



6. LinkedIn

Date: April 2021

Impact: Over 700 million user records

With about 750 million users in 2021, hackers were able to post the user identities of about 700 million people (>93% of the total user base) after performing a data scrape of the LinkedIn website. Although most of the information was publicly available, performing a data scrape by exploiting LinkedIn's API violated the terms of service.

The scraped data included:

- Full names
- Phone numbers
- Email addresses (not publicly available)
- Usernames
- Geolocation records
- Genders

Senders

- Details to linked social media accounts

Any email addresses exposed during a breach can potentially be subject to [ransomware](#) or [phishing](#) attacks. Though the data was publicly available, it raised concerns over information security and how third parties can use that information to create [OSINT \(open-source intelligence\) databases](#).

It also provides an opportunity for bad actors to target high-profile individuals or company executives. For example, smaller hackers quickly tried to piggyback off this incident. One user claimed to sell a new set of LinkedIn data on a public forum in exchange for \$7000 worth of Bitcoin.

JPMORGAN CHASE & CO.

7. JPMorgan Chase

Date: June 2014

Impact: 76 million households & 7 million small businesses

In September 2014, [JPMorgan Chase](#), one of the largest banks in the US, disclosed that cyberattacks compromised accounts of over 76 million households and 7 million small businesses. Although the attack was initially thought to have only affected 1 million accounts, investigations found that the attack was much worse, lasting about a entire month from June to July.

JPMorgan Chase customers luckily didn't suffer any financial fraud, as the data breach was limited to names, emails, and phone numbers. However, further investigations found that the hack also reached JPMorgan servers by stealing a bank employee's identity. Gigabytes of sensitive data were stolen and later linked to a Russian attack by the FBI. Following the incident, JPMorgan executives pledged to spend \$250 million annually to secure their data properly.



8. Home Depot

Date: April 2014

Impact: 56 million payment card numbers & 53 million email addresses

In 2014, hackers were able to steal over 56 million payment card records from [Home Depot](#) using custom-built malware. The attack lasted for five months before it was detected and finally removed from the networks of the popular home improvement store. However, it had already affected millions of customers spanning the US and Canada.

Upon investigation, cybersecurity experts found that the cybercriminals most likely breached the servers through a third-party supplier. Once they

were inside the networks, the hackers were able to install malware on the point-of-sale (POS) systems, allowing them to collect payment card data and upload them to a separate server.

The attack highlighted how little many large retailers spend on cybersecurity to protect sensitive information. By 2020, although Home Depot had significantly improved its payment system protection, it suffered about \$180 million in damages. Much of the damages included payments to credit card companies and banks, court settlements, and customer payouts.



9. MySpace

Date: June 2013

Impact: Over 360 million accounts

Although no longer the social networking site it once was, [MySpace](#) still attracts millions of visitors to their now predominantly music and band promotion site. In 2016, reports came out that a hacker accessed 360 million user logins, names, and dates of birth and posted them for sale on the dark web, making it one of the largest data breaches ever.

Before 2013, MySpace used an **unsalted hash algorithm** to **encrypt user passwords**. The fixed length of this older SHA-1 algorithm made it extremely easy to crack. Newer password authentication protocols use a **salted hash algorithm**, which adds a random string of characters to the end of each encryption.

Luckily, MySpace confirmed that all of the stolen data was from before 2013 when the company rolled out newly updated security measures. They were able to invalidate all of the stolen passwords and notify the affected users of the breach.



10. FriendFinder Networks

Date: November 2016

Impact: 412 million accounts

Popular adult entertainment company FriendFinder Networks faced a massive data breach in 2016 when six of its main databases were hacked, including its more well-known subsidiaries, [AdultFriendFinder](#) and [Penthouse](#). Over 20 years of data were stolen, which amounted to about 412 million accounts, including 15 million deleted accounts that weren't removed from the databases. The breach contained extremely compromising information that included:

- Usernames and passwords
- Email addresses (including government and military)
- User activity and transactions
- Membership details
- IP addresses
- Browser information

According to LeakedSource, FriendFinder Networks secured their passwords with the unsalted hash algorithm SHA-1 and stored user data in plaintext files. Furthermore, a white-hat hacker named Revolver revealed a **Local File Inclusion (LFI)** vulnerability from photos shared on social media. This was a huge security issue for the adult entertainment company because it had been hacked just one year prior, in May 2015, which compromised 3.5 million users. Despite the data breaches, AdultFriendFinder still attracts over 50 million visitors per month worldwide.



11. Marriott International

Date: September 2018

Impact: 500 million guests

On November 19, 2018, [Marriott International](#) released a [statement](#) acknowledging that an unknown third party had illegally accessed their Starwood reservation database. The Starwood database included every reservation made at major hotel chains under Marriott, including Westin, Sheraton, Four Points, St. Regis, and W Hotels.

Upon further investigation, the team at Marriott found that guest data had been copied, encrypted, and duplicated from as far back as 2014. In total, approximately 500 million guests were affected. For about 327 million guests, the hackers were able to steal information that included:

- Names
- Home addresses
- Email addresses
- Phone numbers
- Passport numbers
- Starwood Preferred Guest (SPG) account information
- Date of birth
- Genders
- Reservation details
- Credit card information

For the remaining guests, the stolen data was limited to names, addresses, and emails.

This incident highlighted the lack of data security within the hospitality industry. When Marriott acquired Starwood in 2016, it failed to update the old reservation system, leaving it highly vulnerable to malware and data breaches. Many cybersecurity experts believe that the Chinese government initiated this attack to gain valuable information. In 2019, Marriott was fined almost \$24 million by the UK Information

Commissioner's Office (ICO) for failing to meet cybersecurity standards.



12. Adobe

Date: October 2013

Impact: 38 million credit card numbers

Adobe experienced one of the worst data breaches in the 21st century when sensitive payment card details from approximately 38 million accounts were posted on the dark web. Initially thought to be around 3 million, Adobe's director of security, Brad Arkin, admitted that the number was much higher. The attackers were able to obtain access to information like:

- Adobe user IDs and passwords
- Full names
- Credit/debit card information
- Product source codes (Acrobat, ColdFusion, ColdFusion Builder)

Adobe's main issue was shifting from selling desktop licenses to a cloud-based SaaS company. The transition left them vulnerable due to a lack of IT security, from the servers to the general infrastructure. In addition, Adobe used the same password encryption key for all 38 million affected users, demonstrating poor data protection practices. Adobe settled a lawsuit with 15 states for just \$1 million in 2016.



13. eBay

Date: March 2014

Impact: 145 million users

In 2014, global retailer and auction site eBay was hit with a massive data breach that stole the passwords of 145 million users. Hackers obtained access to the main network by stealing login credentials from just a few eBay employees. Luckily, financial information was stored on a separate server, so the scope of the attack was limited to:

- Full names
- Home addresses
- Email addresses
- Phone numbers
- Date of birth

eBay quickly began to notify their customers to change their passwords to avoid further damage. Although there was no reported financial fraud.

Security First Innovations, LLC, Exhibit 2034

Page 2034 - 10

IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

it's important to note that many people reuse their passwords at least once, meaning it's highly likely that other services may have been compromised.



14. Equifax

Date: September 2017

Impact: 148 million Americans (163 million worldwide)

Equifax, one of the big three credit reporting agencies (TransUnion, Experian, Equifax) in the US, reported a major data breach in 2017, which impacted the personal data of 148 million US citizens. As a company that handles extremely sensitive data, Equifax came under fire due to its negligence and poor security posture.

- The first breach occurred through a third-party web portal, Apache Struts, using a known backend vulnerability. Even though the vulnerability was patched, Equifax failed to update its internal servers, allowing intruders to stay active for 76 days.
- Once the hackers were inside the system, they could easily move from server to server because Equifax didn't implement proper network security or segmentation.
- Equifax allowed its Public Key Infrastructure (PKI) certificate to expire, a routine renewal task that would've allowed the company to detect unusual data movements far sooner.
- Equifax gave users broad permissions, which allowed them to access much more sensitive information than they were allowed. A common security practice employed by many corporations involves the principle of least privilege within a zero-trust model. Implementing these two approaches would have required authentication processes that could've prevented many issues.
- The public did not find out about the breach until more than a month after Equifax discovered it. By that time, top executives at the company had already started to sell their stock, triggering accusations of insider trading.

Equifax ultimately invested more than \$1.4 billion to clean up the damages and rebuild its data protection defense. Two years later, they settled with the FTC, various states and territories, and other authorities for \$575 million.

Is Your Business at Risk of a [Data Breach](#)?

[Find out now →](#)



Security First Innovations, LLC, Exhibit 2034

Page 2034 - 11

IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC



15. River City Media

Date: March 2017

Impact: 1.4 billion file records leaked

One of the world's largest email spam operations, River City Media, suffered one of the world's largest database leaks in US history from 2016 to 2017. This leak exposed the personal details of almost 1.4 billion people and a host of internal company documents. Although most of the information was limited to email addresses, many records included IP addresses, full names, and physical addresses.

While configuring backup servers to its MySQL database, the Portland-based company failed to set up password protection, exposing the entire company. This simple mistake was overlooked for almost three months, which left over a billion people exposed to potential hackers. During these three months, all 1.4 billion accounts were posted to the internet for anyone to view.

Ultimately, River City Media was reported to Spamhaus, an international cybersecurity organization, to blacklist the spam operation. RCM quickly collapsed due to the negative publicity, despite denying their server vulnerability.



16. Target

Date: November 2013

Impact: 41 million payment card records & 70 million customer records

On one of the busiest shopping days of the year, Target became a victim of a third-party data breach during Black Friday 2013. Even with a security system in place, any organization with vulnerable third parties can put itself at high risk for a data breach or cyber attack. In this case, Target used a portal through which third-party vendors could access their data. However, in doing so, this created a vulnerability in which third parties could access Target's own network.

This major data breach allowed the cybercriminals to steal over 41 million credit and debit card records and 70 million customer records. Managing third-party risk should be at the forefront of every company's cybersecurity practices. All it takes is one compromised third party to infiltrate the entire network.

On top of that, Target did not have a segmented network or sufficient firewall in place, which would have greatly limited the cyber attack. Once inside, the hackers used a Trojan to attack Target's point of sale (POS) system, which allowed them to access payment card information.

Ultimately, Target incurred about \$202 million in losses (\$292 million before insurance), which included an \$18.5 million settlement payout, a \$10 million class-action lawsuit, and \$127.5 million paid to banks and credit card companies. They also spent a large sum of money on

Security First Innovations, LLC, Exhibit 2034

Page 2034 - 12

IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

credit card companies. They also spent a large sum of money on [upgrading their cybersecurity practices](#), as listed on their [corporate page](#):

- Improved monitoring of system activity
- Improved firewall
- Whitelisting POS systems
- Adding network segmentation
- Limiting third-party access
- Reduced employee access privileges

Heartland

17. Heartland Payment Systems

Date: May 2008

Impact: Over 100 million payment card records

Heartland, a company specializing in payment, POS, and payroll systems, fell victim to a data breach in 2008, where attackers made off with over 100 million payment card records. However, due to poor security management, the company didn't realize any illegal activity until five months later in October 2008, when Visa and MasterCard reported suspicious transactions from Heartland accounts.

After hiring a cybersecurity forensic team, they found that their systems had been attacked by [SQL injection](#) in 2007, which allowed the hackers to modify web code and gain access to logins. They were able to navigate Heartland systems unimpeded for months and created counterfeit credit cards with real magnetic strips.

Although the culprits were eventually caught, Heartland suffered irreparable damage, losing a large portion of customers and over \$200 million paid out in compensation. Within months of the incident, their stock prices fell 77%. Later in 2015, a larger payment processor, Global Payments, acquired Heartland for \$4.3 billion.



18. Exactis

Date: June 2018

Impact: 340 million people

Exactis, a Florida-based marketing firm that collects and sells data on businesses and consumers, reportedly exposed a database containing 340 million individual records. Initially discovered by security researcher Vinny Troia, he found the entire Exactis database on a public network that was completely unsecured and accessible to everyone.

Troia immediately contacted the FBI, who conducted their own

Security First Innovations, LLC, Exhibit 2034

Page 2034 - 13

IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

investigation. The FBI believed that the database contained information on nearly all US citizens and millions of businesses from their findings. The database contained sensitive data including, but not limited to:

- Full names (including children)
- Age
- Gender
- Physical addresses
- Email addresses
- Religious affiliations
- Political affiliations
- Smoking habits
- Pets
- Income
- Credit rating
- Education level

It was one of the most complete collections of data ever compiled, fully exposed for anyone to view. This information could allow scammers and cybercriminals to execute [social engineering](#) attacks on a widespread level, targeting unsuspecting individuals and businesses with poor security practices.

Although the database was taken off the public domain shortly after it was reported, the FBI believes it was available online for an extended period. Exactis remained silent on the issue but is currently facing multiple class-action lawsuits.



19. Capital One

Date: July 2019

Impact: 100 million user records

In 2019, Paige Thompson, a former Amazon Web Services (AWS) employee, hacked the [Capital One](#) servers and gained access to over 100 million customer account records and credit card applications from as far back as 2005. Of these records, these included:

- Bank account numbers
- Names
- Addresses
- Credit scores
- Account balances
- Social Security numbers
- Canadian Social Insurance numbers

Thompson [exploited a cloud firewall configuration vulnerability](#), which allowed her to execute multiple commands on the Capital One servers. She obtained administrator credentials to bypass the firewall, accessed the data buckets and folders, and copied and exported the data. She then posted the stolen data to GitHub, which created a digital trail that led to her arrest.

Despite being a major advocate for cloud services, Capital One failed to implement sufficient security measures to protect customer data. If Capital One had implemented segmented network security or limited user access privileges, it might have made things much more difficult for Thompson to access. It would have required multiple verification processes for each layer of data.

With more and more companies transitioning to cloud-hosted servers, cybersecurity solutions that monitor the third-party attack surface must be put in place. Capital One would end up settling a class-action lawsuit in 2021 for \$190 million.



20. Dubsmash

Date: December 2018

Impact: 162 million user records

In December 2018, a massive data breach hit 16 different websites, affecting over 617 million stolen accounts. Dubsmash was the most prominent victim, having over 162 million user records compromised on the dark web. The stolen data included:

- Usernames
- Passwords
- Email addresses
- Geolocations
- Country

Companies around the world also suffered major data losses in this same attack, including:

- Under Armour / MyFitnessPal (151 million)
- MyHeritage (92 million)
- Whitepages (18 million)
- Armor Games (11 million)
- Coffee Meets Bagel (6 million)



21. Deep Root Analytics

Date: June 2017

Impact: 198 million US citizens

The personal information of almost 200 million registered voters was leaked in June 2017, data owned by Republican data analysis group Deep

Security First Innovations, LLC, Exhibit 2034

Page 2034 - 15

Root Analytics. The data was first discovered by the cyber threat analysis team at UpGuard, which was the largest exposure of sensitive voter information in history.

The data contained:

- Names
- Addresses
- Emails
- Phone numbers
- Birthdates
- Internet browsing history
- Voter ID numbers
- Political affiliations
- Religions & ethnicities

With this data, political parties on both sides could potentially exploit it to manipulate voter behavior. Many high-profile, influential individuals and organizations were also included in this data set. Although the Republican National Committee (RNC) cut ties with Deep Root Analytics shortly after the data breach, they rehired the data organization in 2020 to prepare for Donald Trump's reelection bid.



22. Zynga

Date: September 2019

Impact: 218 million users

Zynga, one of the most popular online gaming companies, announced a password breach in September 2019 that affected over 200 million users. Through popular mobile games such as Words With Friends, Farmville, and Draw Something, a hacker named Gnosticplayers was able to access the system to steal usernames and passwords.

Despite admitting to the password breach, Zynga failed to notify users immediately. Although no financial information was exposed, this Zynga breach represents a significant concern for hackers to utilize simple information to engineer phishing attacks or scams. If compromised data makes it to the dark web, individuals could potentially be subject to cyberattacks.

Is Your Business at Risk of a [Data Breach?](#)

Find out now →



23. Progress Software (MOVEit vulnerability)

Date: June 2023

Impact: 94 million users / >2500 organizations / >\$15 billion in damages

In one of the more high-profile attacks in 2023, the [MOVEit vulnerability](#) was a zero-day vulnerability that affected many of the world's largest organizations. The vulnerability originated from [Progress Software's](#) file transfer application, MOVEit Transfer, a software that thousands of organizations around the world use.

Although the breach occurred worldwide, it's estimated that nearly 80% of MOVEit victims were US corporations, which included the US Department of Energy, First National Bank, University of Georgia, Johns Hopkins University, NYC Department of Education, and more.

The initial MOVEit vulnerability was one of eight CVEs disclosed by Progress Software, and many organizations are still dealing with the fallout and recovery from the zero-day. As of early 2024, the number jumped to over 94 million users impacted and over \$15 billion in total damages, and still counting.

[Learn more about the MOVEit zero-day vulnerability >](#)



24. Plex

Date: August 2022

Impact: 30 million users

[Plex](#), a media streaming platform, issued password-reset notices to nearly all 30 million users on August 24th, 2022, after noticing that [an unauthorized party had accessed data](#) that included emails, usernames, and encrypted passwords. Although passwords were encrypted with a hashing algorithm to prevent the likelihood of criminals stealing accounts, the [data breach](#) exposed an unpatched [vulnerability](#) that allowed the criminal to tunnel their way into Plex's systems.

Furthermore, the widespread password changes exposed Plex's inability to handle the traffic on their internal servers, creating additional error messages or failed password changes. Even with encrypted passwords, threat actors can utilize [brute-force](#) encryption-cracking software to steal basic passwords that many people use.

Because no payment information was stored on Plex servers and the company responded quickly to the situation, there were ultimately no penalties or cases of stolen information. The incident highlights the importance of [creating strong passwords](#) in case of an attack.



Security First Innovations, LLC, Exhibit 2034

Page 2034 - 17

IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

UNIFIED

25. Los Angeles Unified School District (LAUSD)

Date: September 2022

Impact: 1000 schools / 600,000 students / 500GB of data

In one of the [biggest data breaches of all time in the education industry](#), the [Los Angeles Unified School District \(LAUSD\)](#) was attacked by a Russian criminal group, Vice Society, over Labor Day weekend. The attack affected over 1000 schools and 600,000 students in the second-largest school district in the United States. Vice Society deployed a ransomware attack that prevented LAUSD officials from accessing critical data, including:

- Personal information (names, physical addresses, phone numbers)
- Email addresses
- Computer systems and applications
- Passport details
- Employee social security numbers
- Employee account login information
- Tax forms
- Contracts and legal documents
- Financial reports
- Banking details
- Health information (including COVID-19 vaccination data)
- Background checks and conviction reports
- Student psychological assessments
- VPN credentials

Because cybersecurity experts and law enforcement strongly advise against paying ransoms, LAUSD released a statement that announced they would not be paying the ransom given to them. As a result, Vice Society published the [stolen data](#) on their [dark web](#) forum.

Although the lasting impact of the attack has yet to be determined, potential lawsuits could be on the horizon if cases of fraud or [identity theft](#) become prevalent. It's also important to note that the LAUSD [was notified of potential vulnerabilities prior to the attack](#) and failed to resolve or remediate the issues, which could result in further penalties or fines after investigation.



26. Cash App

Date: April 2022

Impact: 8.2 million users

In April 2022, information from over 8 million users was downloaded by a former disgruntled employee through [Cash App Investing](#), a stock trading feature accessible through CashApp's service. It's important to note that

Security First Innovations, LLC, Exhibit 2034

Page 2034 - 18

IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

information held through Cash App Investing is separate from Cash App's main product of person-to-person payment service.

Information that was stolen included:

- Customer names
- Brokerage account numbers
- Stock trading portfolios
- Stock trading activity

Although no other personally identifiable information (PII) was stolen, the data breach was a significant security risk reflecting a failure to implement access control policies, especially for an employee who no longer worked at Cash App. Moreover, the attack continued to happen over a 4-month period while Cash App failed to detect or act on the active data breach.

After the illegal downloading of sensitive information, Cash App is currently undergoing multiple class-action lawsuits for failing to implement proper security measures to protect user data.

■ Free resource

A Complete Guide to Data Breaches

Learn how to avoid a costly data breach with a comprehensive prevention strategy.





Download now

Experience superior visibility and a simpler approach to cyber risk management

Get a demo

Free trial



Platform	Products		Compare	Resources	Company
Reporting	 Vendor Risk	 Breach Risk	BitSight	News	About us
Services	 User Risk	 Trust Exchange	SecurityScorecard	Events	Careers
Security ratings			CyberGRX	Breaches	Contact
Integrations			RiskRecon	Templates	Press
			All comparisons		Support
					Security
			Solutions	Quick links	Tools
			Financial Services	Third-Party Risk Management	Security Reports
			Technology	Attack Surface Management	Instant Security Score
			Healthcare		

© 2025 UpGuard, Inc [X](#) [in](#) [f](#) [G](#) [v](#) [y](#) [Website Terms & Conditions](#) [Platform Terms & Conditions](#) [Research Guidelines](#) [Cookies](#) [Privacy](#)

Do not sell or share my personal information