# The Top 10 Data Breaches of 2024

BY YANNICK MERCKX · DECEMBER 24, 2024 · LAST UPDATED ON MARCH 6, 2025

2024 has been a tumultuous year in cybersecurity with numerous significant data breaches compromising sensitive information and affecting millions globally. While these breaches have caused significant harm, they offer an opportunity to learn and strengthen your defenses.

These incidents underscore the importance of resilient and strong cybersecurity measures. Below, we explore the top 10 data breaches of the year, detailing their causes, impacts, and the responses from the organizations involved.

## 1. National Public data breach

In August 2024, National Public Data (NPD), a company specializing in employee background checks, suffered a massive data breach. Hackers accessed sensitive personal information, including Social Security numbers, affecting nearly all Americans.

- **Industry:** Data Broker
- **Breach Size:** 2.9 billion records

**Impact and Response**

The breach led to dozens of lawsuits alleging negligence and breaches of fiduciary duty. NPD acknowledged the breach and cooperated with law enforcement. Affected individuals were advised to monitor their financial accounts and place fraud alerts with credit reporting agencies. In October 2024, Jerico Pictures Inc, doing business as NPD, filed for Chapter 11 bankruptcy as it currently faces over a dozen lawsuits over the breach.

## 2. Snowflake Inc. breach

In mid-2024, Snowflake Inc., a cloud-based data warehousing company, experienced a significant breach. The hackers gained access by exploiting unencrypted usernames and passwords stored on a worker's computer and in a project management tool named JIRA. Using these credentials, they were able to infiltrate several Snowflake customer accounts, such as Ticketmaster and Santander, resulting in a huge fall-out.

- **Industry:** Cloud Data Warehousing
- **Breach Size: Impacted the data of 165+ customer** (i.e AT&T, Ticketmaster, Santander Bank,...)

**Impact and Response**

The breach potentially became one of the largest ever, with criminals making passwords for hundreds of Snowflake accounts available online. Investigations revealed the use of infostealer malware to obtain

login credentials, exploiting accounts lacking multi-factor authentication (MFA). Snowflake has since enabled MFA by default for all user accounts to enhance security.

The data breach also exposed a significant number of organizations across various industries. Mandiant researchers identified approximately 165 potentially compromised organizations, with multiple high-profile companies experiencing substantial data breaches due to inadequate multi-factor authentication (MFA) practices.

Exposed organizations include:

- **AT&T:** 50 billion records breached, being nearly all wireless customers, with data including phone numbers and call records.
- **Ticketmaster:** Over 500 million individuals breached, exposing personal and payment information.
- **Advance Auto Parts:** Over 2.3 million individuals breached, compromising names, Social Security numbers, and driver's license numbers

# 3. Change Healthcare breach

Change Healthcare, a crucial healthcare technology infrastructure company that processes between one-third and one-half of all U.S. healthcare transactions, suffered a catastrophic ransomware attack by the BlackCat/ALPHV group. The breach occurred through compromised credentials of a low-level customer support employee who lacked multi-factor authentication. This incident resulted in one of the largest healthcare data breaches in U.S. history, affecting approximately 100 million Americans, making it a historically significant cybersecurity event impacting roughly one-third of the entire U.S. population.

- **Industry**: Healthcare Technology/Services
- **Breach Size:** 100 million records (approximately one-third of the U.S. population)
- **Financial impact:** $2.457 billion, with $1.521 billion in direct breach response costs.

**Impact and Response**
The breach's impact was unprecedented in both scope and financial damage. The compromised data included comprehensive personal, financial, and healthcare records, encompassing:

- Medical record numbers, diagnoses, medications, and treatment details
- Payment card information and banking records
- Social Security numbers and driver's license numbers
- Insurance information and member ID numbers

The financial impact on UnitedHealth Group, Change Healthcare's parent company, reached $2.457 billion, with $1.521 billion in direct breach response costs. This incident has become a watershed moment for cybersecurity in healthcare, prompting industry-wide reassessment of security protocols, particularly regarding authentication measures and access controls. The scale and scope of this breach have led to increased scrutiny of healthcare sector cybersecurity practices and infrastructure resilience.

# 4. MediSecure breach

In May 2024, MediSecure, an Australian prescription company, experienced a breach that exposed patient records, including medical histories and personal identification information.

- **Industry:** Healthcare Data Management
- **Breach Size:** Patient records of **12.9 million individuals**

**Impact and Response**

The breach is marked a one of the biggest cyberattacks in Australian history. Medisecure was one of only two eScript providers in Australia until late 2023 year, when competitor eRx took over the government contract to supply the entire market .

# 5. Internet Archive breach

The Internet Archive, a digital library, suffered a data breach in October 2024, compromising user account information and email addresses.

- **Industry**: Digital Library and Web Archiving
- **Breach Size: 31 million unique records**, including email addresses, screen names, and bcrypt-hashed passwords

**Impact and Response**

The organization promptly informed users, urging them to change passwords and enabling two-factor authentication. They also conducted a thorough security audit to identify and rectify vulnerabilities.

# 6. Halliburton cyberattack

Halliburton, an oilfield services company, was targeted by a cyberattack that disrupted operations and led to unauthorized access to corporate data.

- **Industry**: Oil and Gas Services
- **Breach Size**: Undisclosed
- **Financial Impact:** $35 million in losses

**Impact and Response**

The attack caused operational delays and potential exposure of proprietary information. They even had to proactively take certain systems offline to protect them, limiting access to portions of its business application. Halliburton collaborated with cybersecurity experts to restore systems and implemented advanced threat detection measures.

# 7. Dell Technologies breaches

Dell Technologies experienced multiple data breaches that exposed employee records and internal company information in 2024. The incidents occurred in quick succession, highlighting significant vulnerabilities in the company's security infrastructure.

• **Industry**: Technology and Computing

• **Breach Size**: Approximately **10,863 employee records** in the first breach, with additional data compromised in a second breach. This is affecting potentially up to 49 million customers

Impact and Response

The breach was particularly notable as it occurred in two waves. The first incident involved a threat actor known as "Grep" who leaked employee information. Days later, a second breach occurred when attackers allegedly compromised Dell's Atlassian account. Dell initiated investigations into both incidents and began notifying affected employees. The total compromised data amounted to approximately 3.5GB of internal information. Some reports indicate the potential impact on up to 49 million users, though Dell is still investigating this number.

# 8. Ivanti Zero-Day incident

Ivanti disclosed multiple zero-day vulnerabilities in its Connect Secure and Policy Secure VPN appliances, leading to one of the most significant cybersecurity incidents of the year. The vulnerabilities allowed unauthorized access and remote code execution, affecting organizations globally including government agencies.

- **Industry:** Cybersecurity/Network Security
- **Breach Size:** Over **28,000 instances exposed across 145 countries**, with more than 600 confirmed compromised cases

Impact and Response

The breach was particularly severe as it affected critical infrastructure and government agencies, including CISA (Cybersecurity and Infrastructure Security Agency). The attack chain involved multiple vulnerabilities (CVE-2023-46805, CVE-2024-21887, and CVE-2024-21893) that could be exploited together. Threat actors were able to breach email accounts at approximately 25 organizations, including government entities. CISA was forced to take systems offline, and Ivanti issued multiple security patches throughout the year. The incident led to a massive remediation effort across affected organizations, with some completely replacing their VPN infrastructure.

# 9. LoanDepot incident

LoanDepot, one of America's largest non-bank retail mortgage lenders, suffered a major ransomware attack that severely disrupted its operations and affected millions of customers. The ALPHV/BlackCat ransomware group claimed responsibility for the attack.

- **Industry**: Financial Services/Mortgage Lending

- **Breach Size**: **16.6 million individuals** affected
- **Financial Impact: $27 million in direct costs** to the company

**Impact and Response**

The attack led to widespread system outages that prevented customers from accessing their accounts and making mortgage payments. Key systems were taken offline, including loan processing and phone services. The breach compromised sensitive personal information of approximately 16.6 million individuals, including Social Security numbers and other critical personal data. The company was forced to implement manual workarounds for payment processing and customer service operations.

# 10. Evolve Bank & Trust breach

- **Industry:** Financial Services
- **Breach Size:** 7.6 million records

Evolve Bank & Trust, a prominent banking-as-a-service company based in the United States, **disclosed a significant data breach affecting 7.6 million individuals.** The breach, attributed to the LockBit ransomware group, exposed sensitive personal information of Evolve's customers, employees, and clients of its fintech partners.

**Impact and Response**

The compromised data included names, Social Security numbers, bank account details, and contact information of personal banking clients. Additionally, the breach affected customers of Evolve's fintech partners, including Affirm, Mercury, and Wise. In response to the incident, Evolve initiated an investigation and is offering two years of credit monitoring and identity protection services to affected U.S. residents, as well as dark web monitoring for international customers.

# FAQs

**1. How can Intigriti help prevent data breaches?**

Intigriti is a crowd-sourced security platform that connects organizations with ethical hackers worldwide. These experts identify vulnerabilities and provide actionable insights, enabling companies to patch security gaps before attackers can exploit them.

**2. Why are crowd-sourced security platforms effective?**

Crowd-sourced platforms tap into a global network of ethical hackers, providing diverse perspectives and innovative solutions to security challenges. This approach ensures that vulnerabilities are discovered and addressed faster.

**3. How can affected individuals confirm if their data was involved in a breach?**

Services like Have I Been Pwned or direct communication from the affected organization can help individuals check if their data was compromised. Always rely on official sources and avoid phishing scams that exploit breach notifications.

**REQUEST A DEMO**

intigriti.com/demo

**VISIT THE WEBSITE**

intigriti.com

**GET IN TOUCH**

hello@intigriti.com