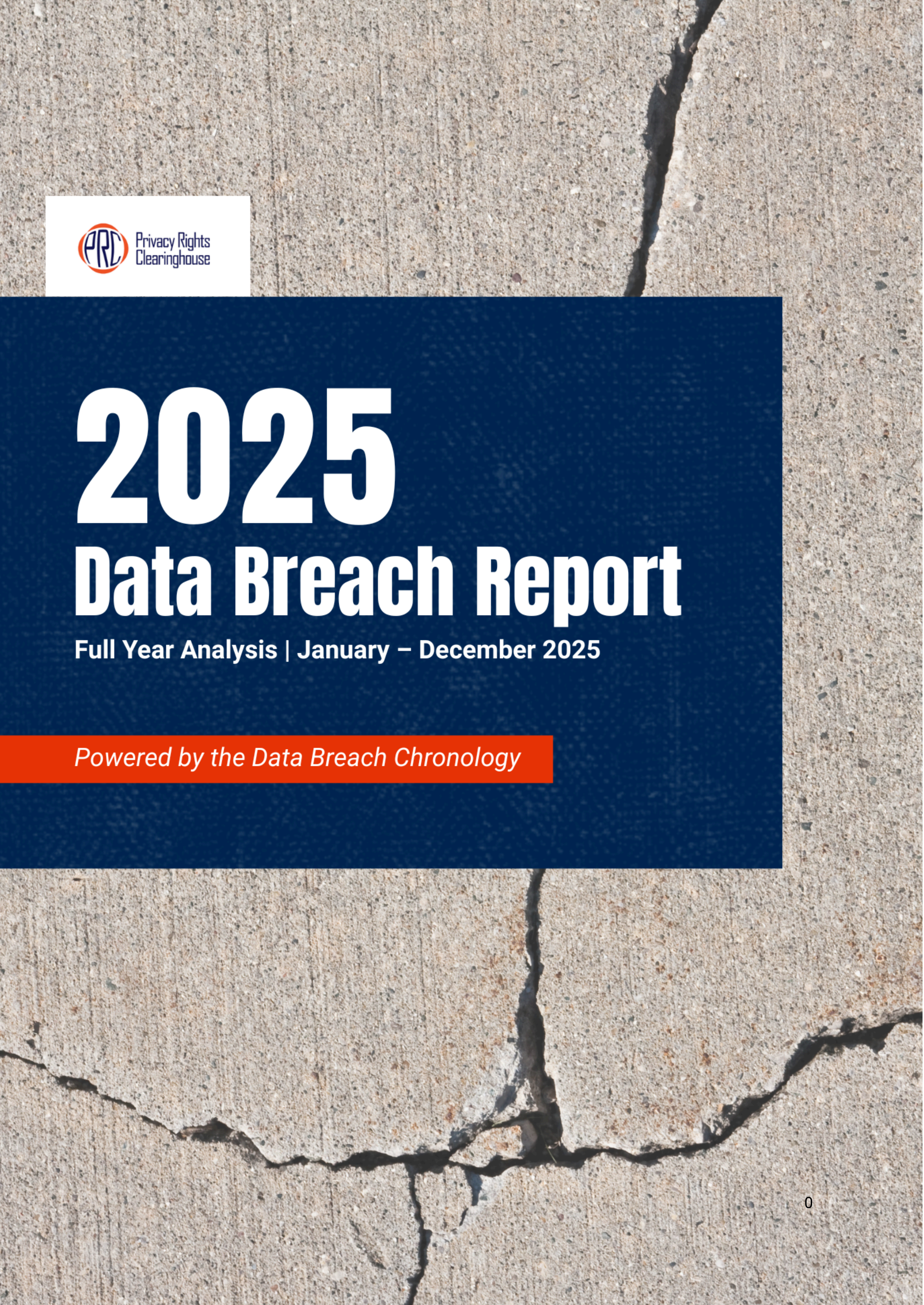


Privacy Rights Clearinghouse

2025 Data Breach Report

Full Year Analysis | January – December 2025

Powered by the Data Breach Chronology

Executive Summary

In 2025, state attorneys general and the U.S. Department of Health and Human Services shared 8,019 data breach notification filings reported to their offices. These represented 4,080 unique breach events impacting at least 375 million individuals.

The year's statistics were dominated by Change Healthcare, whose final notification of the year arrived in October, twenty months after the February 2024 ransomware attack, confirming 192.7 million people were affected. It's the largest healthcare data breach ever recorded, more than double the Anthem breach that held that record for a decade, and it accounts for more than half of the year's 375 million affected.

Among reported breaches that occurred in 2025, the largest was Prosper Marketplace, a peer-to-peer lending platform whose systems were compromised between April and September, exposing 13.1 million borrowers' financial information. Other major 2025 breaches included Episource , a healthcare technology company hit by ransomware (6.6 million in January); 700Credit, a company that processes credit checks for thousands of auto dealerships nationwide (5.8 million in October); TransUnion, one of the big three credit reporting agencies (4.5 million in July), and the U.S. Department of Treasury (2.4 million in January).

Healthcare organization breaches accounted for 249 million of the 375 million individuals reported in 2025 breach filings, or 66% of the total. Change doHealthcare alone accounts for more than three-quarters of the 249 million. Major health system breaches first disclosed in 2025 included Yale New Haven Health (5.6 million, first reported in April) and Blue Shield of California (4.7 million, first reported in April). Ascension Health's 2024 ransomware attack (5.5 million in May 2024) also continued generating notifications into 2025. Business service providers appeared throughout the data as well: Conduent (10.8 million in October 2024), Infosys McCamish (6.1 million in October 2023), and VeriSource Services (4.1 million in February 2024) all disclosed breaches or continued reporting on prior incidents affecting millions of their clients' customers. In the education sector, PowerSchool's December 2024 breach generated notifications throughout 2025 as K-12 districts across the country discovered the scope of student data exposure.

Beyond these figures, this report examines gaps in data breach reporting. Notifications rarely explained with specificity how attackers gained access. More than half of the 2025 notifications came from state agencies that publish only summary data rather than the underlying notification letters. Where letters were available, only 17% mentioned a specific attack method. Notifications also arrived long after breaches occur, with the most common window being 91 to 180 days for breaches with both reported date and breach date available to compare.

Table of Contents

I. ABOUT THE DATA BREACH CHRONOLOGY

Privacy Rights Clearinghouse is a nonprofit organization focused on increasing access to information, policy discussions and meaningful rights so that data privacy can be a reality for everyone. Our organization was founded in 1992 and has tracked data breach notifications since 2005. The Data Breach Chronology is Privacy Rights Clearinghouse's database of publicly reported breaches, aggregating notification filings from 15 state attorneys general offices and the U.S. Department of Health and Human Services.

The Data Breach Chronology serves researchers, journalists, regulators, legal scholars, and security professionals studying patterns in data privacy and security. It has been broadly used for academic research on breach impacts, regulatory enforcement, and the economics of data security.

Anyone is free to explore the Data Breach Chronology at privacyrights.org/data-breaches, where users can search, filter, and browse breach records going back to 2005. For researchers, journalists, and organizations that need the complete dataset, the full Chronology is available for download at store.databreachchronology.org.

Purchases of the database, grants, cy pres awards, and individual donations directly support continued development, maintenance, and expansion of the Data Breach Chronology. They also allow us to continue providing complimentary access to researchers working to advance consumer privacy and security.

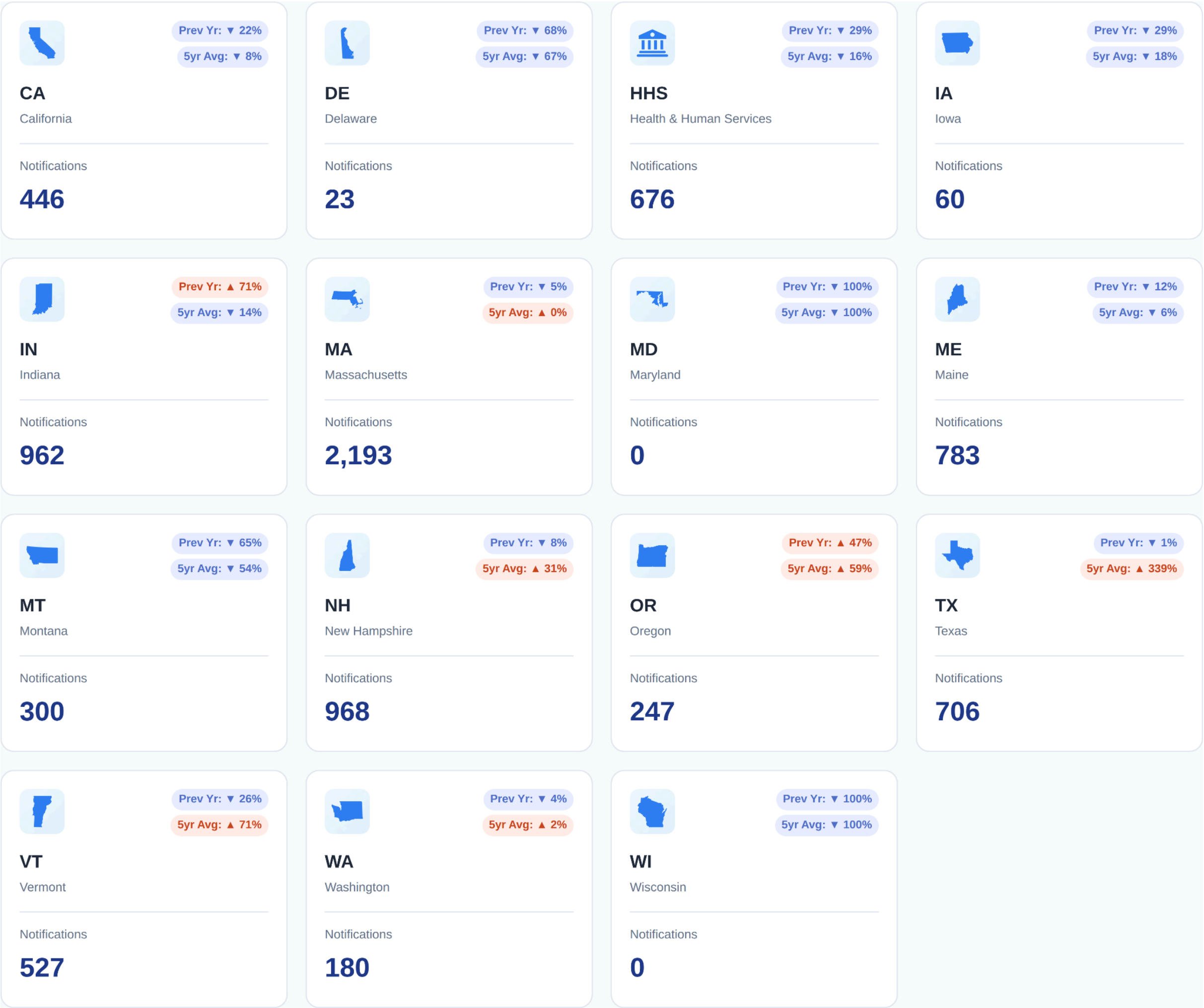
Methodology

The Data Breach Chronology captures information organizations are required to report to agencies that then publicly disclose this information; it does not represent all data security incidents. Many breaches go unreported, particularly those affecting fewer individuals than state reporting thresholds require.

Also, the Data Breach Chronology only contains information present in these publicly reported filings; there may be more information reported through the media or on the breached organization's website that wouldn't be included in this analysis. Any breach-specific information in this report that isn't otherwise cited comes directly from these notification filings.

When a single breach generates notifications in multiple states, or multiple notifications are sent out about a single breach as more information is discovered, we attempt to cluster those filings together and report them as one event, using the maximum affected count reported across those filings to assess the number of individuals impacted. The impact totals in this report sum these event-level figures. This is not a unique headcount. The same person affected by multiple breaches is counted multiple times, and there is currently no way for us to identify or adjust for this overlap. The figures measure how many times personal information was exposed, not how many distinct people were affected.

Data Sources for 2025



Prev Yr: ▼ 22%
5yr Avg: ▼ 8%
CA
California
Notifications
446

Prev Yr: ▼ 68%
5yr Avg: ▼ 67%
DE
Delaware
Notifications
23

Prev Yr: ▼ 29%
5yr Avg: ▼ 16%
HHS
Health & Human Services
Notifications
676

Prev Yr: ▼ 29%
5yr Avg: ▼ 18%
IA
Iowa
Notifications
60

Prev Yr: ▲ 71%
5yr Avg: ▼ 14%
IN
Indiana
Notifications
962

Prev Yr: ▼ 5%
5yr Avg: ▲ 0%
MA
Massachusetts
Notifications
2,193

Prev Yr: ▼ 100%
5yr Avg: ▼ 100%
MD
Maryland
Notifications
0

Prev Yr: ▼ 12%
5yr Avg: ▼ 6%
ME
Maine
Notifications
783

Prev Yr: ▼ 65%
5yr Avg: ▼ 54%
MT
Montana
Notifications
300

Prev Yr: ▼ 8%
5yr Avg: ▲ 31%
NH
New Hampshire
Notifications
968

Prev Yr: ▲ 47%
5yr Avg: ▲ 59%
OR
Oregon
Notifications
247

Prev Yr: ▼ 1%
5yr Avg: ▲ 339%
TX
Texas
Notifications
706

Prev Yr: ▼ 26%
5yr Avg: ▲ 71%
VT
Vermont
Notifications
527

Prev Yr: ▼ 4%
5yr Avg: ▲ 2%
WA
Washington
Notifications
180

Prev Yr: ▼ 100%
5yr Avg: ▼ 100%
WI
Wisconsin
Notifications
0

Figure 1. Notification counts by source for 2025, with year-over-year and five-year average comparisons. The Data Breach Chronology aggregates filings from 14 state attorneys general offices and the U.S. Department of Health and Human Services. Maryland and Wisconsin, which previously shared data, did not publish notifications in 2025.

II. SUPPORTING PRIVACY RESEARCH

One of the most rewarding parts of maintaining the Data Breach Chronology is seeing how researchers use it. In 2025, we granted 63 requests for complimentary research access from 56 institutions across 14 countries—Australia, Brazil, Canada, China, France, Germany, Hong Kong, Ireland, Netherlands, Spain, Switzerland, Taiwan, the United Kingdom, and the United States. The researchers came from economics departments, business schools, law schools, and public policy programs as often as from cybersecurity programs.

The questions they're pursuing reflect how deeply data breaches have become embedded in economic and corporate life. Economists are modeling how breaches propagate through supply chains and affect market concentration. Finance researchers are studying whether ESG scores or CEO characteristics predict breach vulnerability. Legal scholars are examining which breach types lead to class action litigation and how often victims receive compensation.

One Australian research team is building a macroeconomic model that predicts mid-sized firms face the greatest cyber risk, as they are often large enough to be attractive targets, but too small to afford sophisticated defenses. A team at the University of Michigan is combining Data Breach Chronology data with federal surveys to estimate how often a breach results in identity theft for affected individuals. A Harvard Law researcher is studying enforcement gaps, noting that roughly 75% of ransomware attacks are estimated to go unreported. A high school student in California is building actuarial models for a national competition.

We're proud the Data Breach Chronology has found its way into research programs around the world. Privacy Rights Clearinghouse has been tracking breaches for twenty years and educating consumers about their rights for more than thirty. The Data Breach Chronology exists because of the researchers, journalists, and organizations who support it.

III. 2025 AT A GLANCE

Metric	2025 Full Year
Total Notification Records	8019
Unique Breach Events	4080
Total Individuals Affected	**374,948,966**

These figures include all breach events with notifications filed in 2025, whether the breach was first disclosed in 2025 or in a prior year with supplemental filings continuing into 2025.

Quarter	Notifications Filed	Events	Total Affected
Q1 (Jan-Mar)	2,213	1,174	50.4 M
Q2 (Apr-Jun)	2,218	1,214	44.3 M
Q3 (Jul-Sep)	1,943	1,039	227.0M
Q4 (Oct-Dec)	1,645	942	53.2 M

The Q3 spike reflects Change Healthcare, whose July notification confirmed the final count of 192.7 million people affected, of Q3's 226 million total. Absent that single event, 2025's quarterly totals would have ranged roughly 35-55 million affected per quarter, reflecting the steady background rate of breach activity.

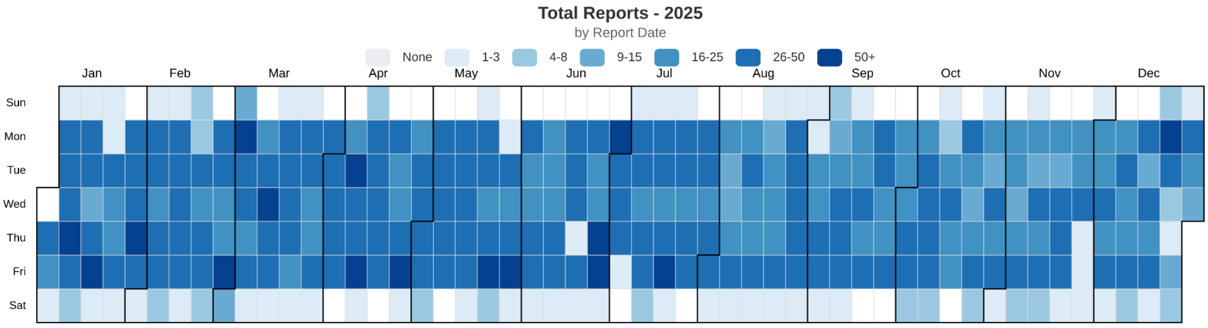


Figure 2. Daily notification volume throughout 2025. Reporting clusters heavily on weekdays (97.5%), with Fridays consistently the busiest. Volume was higher in the first half of the year, tapering after July.

Historical Context

Year	Notifications Filed	Events (First Reported)	Total Affected (First Reported)
2025	8,019	3,892	148.4 million
2024	10,790	4,184	680.2 million
2023	10,070	4,009	485.0 million
2022	8,589	3,757	199.0 million
2021	9,094	3,935	231.2 million
2020	6,706	3,317	160.5 million

Unlike the 2025 summary above, which includes all notifications filed during the year regardless of when a breach was first disclosed, this historical view attributes each breach event and its total affected count to the year of first notification. This avoids double-counting incidents like Change Healthcare, which generated notifications in both 2024 and 2025 but is counted only in 2024 when it was first reported.

The notification counts in 2023 and 2024 were inflated by the MOVEit file transfer vulnerability discovered in May 2023, which generated over 1,000 separate notifications as hundreds of organizations disclosed breaches stemming from the same exploit. The 680 million figure for total affected individuals in 2024 was driven largely by three breaches: National Public Data (270 million), Change Healthcare (193 million), and AT&T (76 million).Looking at 2020–2022 and 2025, total affected has ranged from 148 to 231 million annually, with breach events holding relatively steady at 3,300–4,200 per year.

2025 Breach Notifications Weekly Timeline

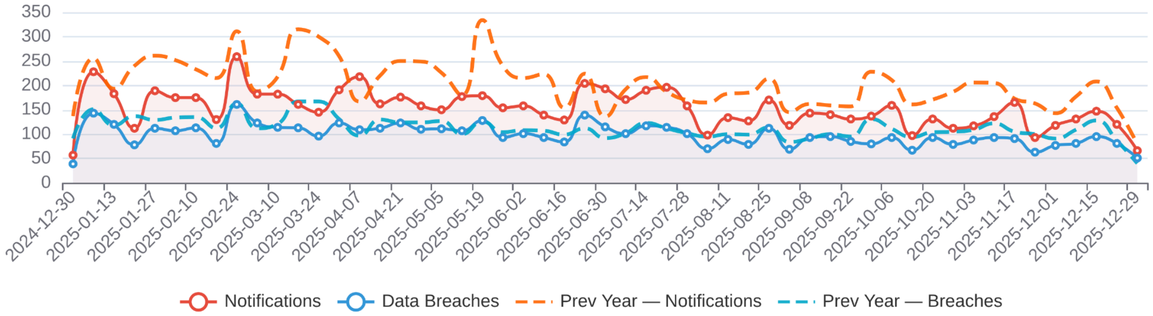


Figure 3. The gap between notifications and unique events reflects multi-state reporting requirements, extended investigations, and supplemental disclosures as organizations discover the full extent of breaches over time. The dotted lines indicate the five year average.

IV. THE BIGGEST STORIES OF 2025

Change Healthcare: The Healthcare System's Single Point of Failure

192.7 million affected | Breach: February 17-20, 2024 | Reported: July 2024–October 2025

By the time Change Healthcare filed its last notification of 2025 in October, it confirmed its February 2024 ransomware attack had exposed the protected health information of approximately 192.7 million people—roughly 57% of the U.S. population. The attack, attributed to the ALPHV/BlackCat ransomware group, exploited compromised credentials to access a Citrix portal that lacked multi-factor authentication.

The breach window was short—four days, from February 17 to February 20, 2024—but the impact was catastrophic. Change Healthcare operates as a healthcare claims clearinghouse, processing billions of transactions annually between healthcare providers and insurance companies.

The final notification letter, spanning 21 pages, included a spreadsheet listing hundreds of covered entities whose patient data flowed through Change Healthcare's systems. Major health systems like CVS Health, Molina Healthcare, Humana, UnitedHealthcare, and Cigna appeared on the list. The compromised data included contact information, health insurance details, medical records, billing information, Social Security numbers, and government ID numbers. Change Healthcare offered two years of credit monitoring through IDX, though the notification acknowledged that "the data that may have been seen and taken was not the same for everyone."

Prosper Marketplace: When the Lender Gets Breached

13.1 million affected | Breach: April–September 2025 | Reported: December 2025

Prosper Marketplace s borrowers with investors willing to fund personal loans.[1] When borrowers apply, they provide information a lender uses to assess risk: Social Security numbers, bank account information, income details, dates of birth. When Prosper discovered unauthorized activity on September 1, 2025, attackers had been querying its databases for four months.

[1] https://www.prosper.com/about

The breach notification, filed in December, confirmed that 13.1 million individuals had their information exposed, making it the largest reported breach that occurred in 2025. The compromised data included names, Social Security numbers, bank account numbers, dates of birth, and other financial information submitted during the loan application process. Prosper's notification stated there was "no evidence of unauthorized access to customer accounts or funds," but the exposed data represents everything needed for identity theft and financial fraud.

The breach lasted roughly four months, from late April through early September, followed by a three-month period before any notification. Affected borrowers potentially spent more than seven months unaware that their financial data had been compromised. Prosper offered two years of credit monitoring through Experian.

700Credit: An Auto Industry Data Broker

5.8 million affected | Breach: October 25–27, 2025 | Reported: December 2025

When a person applies for financing at a car dealership, the dealer runs their credit. For thousands of dealerships across the country, that credit check flows through 700Credit, one of the largest providers of credit reports and identity verification services to the auto industry.[2] In late October 2025, attackers accessed 700Credit's web application and copied customer records over a three-day window.

The 5.8 million people affected weren't 700Credit's customers—as is the case with so many data broker breaches, it is very possible the victims had never heard of the company. Names, addresses, Social Security numbers, and dates of birth were exposed, and 700Credit notified the FBI and FTC and filed notifications with state attorneys general on behalf of the affected dealerships

TransUnion: The Credit Bureau Gets Breached (Again)

4.5 million affected | Breach: July 28, 2025 | Reported: August 2025

TransUnion disclosed in August 2025 that a third-party application serving its U.S. consumer support operations had been compromised, and revealed that names, dates of birth, and Social Security numbers for 4.5 million people had been exposed. The company's notification noted that "no credit reports or core credit information" were accessed.

[2] https://www.700credit.com/about/

However, the exposed data included names, dates of birth, and Social Security numbers; all building blocks of identity theft. TransUnion offered 24 months of credit monitoring through its own myTrueIdentity service.

A credit bureau, whose business model depends on collecting and securing consumer data, suffering a breach and then offering its own credit monitoring service as a remedy captures something about the circular absurdity of our current data security landscape.

This is not new for the credit reporting industry. The Data Breach Chronology has recorded 44 separate breach events at the three major credit bureaus since 2009, generating 185 state notification filings. Equifax's 2017 breach exposed 145.5 million Americans, or roughly 44% of the country. Experian exposed 15 million T-Mobile customers in 2015. TransUnion itself appears in the database repeatedly: credential stuffing attacks affecting nearly 23,000 people in 2020-2022, unauthorized access incidents in 2017-2018 affecting 7,500, and a 2023-2024 breach at its Risk and Alternative Data Solutions subsidiary affecting 87,000.

Conduent: When A Vendor's Vendor Gets Breached

10.8 million affected | Breach: October 21, 2024 - January 13, 2025 |
Reported: October–December 2025

Conduent Business Services provides back-office support to corporations and government agencies, providing printing, mailroom services, document processing, and payment integrity. When attackers gained access to Conduent's network in late October 2024, the breach included files associated with Conduent's clients, who in turn had data from their own customers.

The breach was discovered January 13, 2025, meaning attackers had nearly three months of access. The notification process stretched through 2025, with Conduent filing supplemental notices as it identified additional affected individuals. The final filing of 2025 reported over 10.7 million affected nationwide.

The Conduent breach illustrates the challenge of modern data supply chains: organizations often don't know where their data flows or who ultimately holds it. It is unlikely that individuals affected by this breach have never heard of Conduent, yet their Social Security numbers, medical information, and health insurance details were exposed through a vendor relationship several layers removed from their direct interactions with healthcare providers or employers.

Episource: Healthcare’s Vendor Problem

6.6 million affected | Breach: January 27 - February 6, 2025 | Reported: June–December 2025

Episource is a healthcare technology company that provides services to doctors, health plans, and other health organizations. On February 6, 2025, Episource discovered unusual activity in its systems and determined that attackers had accessed and copied data over the previous ten days.

The compromised information followed a familiar healthcare breach pattern: names, addresses, phone numbers, email addresses, health insurance data including plan and member ID numbers, medical information including diagnoses and treatments, dates of birth, and in some cases Social Security numbers. The notification letters went out to individuals whose data flowed through Episource's systems via their health plans—Molina Healthcare, Community Health Plan of Washington, Humana, Regence, and others.

PowerSchool: Education's Data Problem

877,000+ confirmed across multiple districts | Breach: December 19-28, 2024 | Reported: January–May 2025

PowerSchool provides student information systems to thousands of school districts across North America.[3] When attackers breached its systems in late December 2024, they gained access to sensitive data about students, families, and staff at schools nationwide. A filing in California noted that exposed data could include student names, state IDs, dates of birth, enrollment information, home addresses, parent and guardian contact information, emergency contacts, and medical alerts.

Independent reporting in January 2025 suggested the breach may have affected as many as 62 million students and 9.5 million teachers.[4] Yet the public notification filings tell a different story, not because the numbers are smaller, but because they're largely absent. The largest single notification we identified was Texas, reporting approximately 800,000 affected individuals. Iowa reported nearly 50,000. We also identified ten additional school districts

[3] https://www.powerschool.com/news/powerschool-readies-thousands-of-school-districts-across-the-united-states-for-the-new-school-year/

[4] https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/

that filed their own breach notifications explicitly referencing the PowerSchool incident, adding roughly 27,000 more confirmed affected individuals. Most filings listed the number of affected individuals as unknown. Even combining PowerSchool's direct filings with these district-level notifications, the total confirmed affected is less than 900,000, a fraction of the tens of millions reported in the press.

The notifications themselves explain the gap. According to filings made in Iowa, PowerSchool filed on behalf of "hosted" customers whose data resided on PowerSchool's cloud environment, but many districts host their own data on premises. According to the notifications,the on-premises customers "are not included in PowerSchool's notice because PowerSchool does not have access to relevant data, which resides on those customers' internal systems."

The PowerSchool breach highlights several problems. First, the concentrated risk in educational technology: a single vendor serves thousands of schools, and when that vendor is compromised, children across the country are exposed to identity risks that may follow them for decades. Second, the opacity of breach disclosure. PowerSchool created a dedicated incident response website with FAQs, timelines, and enrollment links for credit monitoring.[5] Nowhere on that page does it disclose how many people were affected. Students, families, and educators are left relying on journalistic estimates to understand the scale of the breach that exposed their data.

U.S. Department of Treasury: Government Data at Risk

2.4 million affected | Breach: January 31, 2025 | Reported: February 2025

Federal agencies aren't immune to data breaches. The U.S. Department of Treasury reported in February 2025 that an internal system breach on January 31 had exposed data for 2.4 million individuals. The breach was discovered within a week, but the damage was done—another reminder that even the organizations responsible for national security and financial oversight face the same vulnerabilities as the private sector.

[5] https://www.powerschool.com/security/sis-incident/

2025 Breaches by Scale and Sector

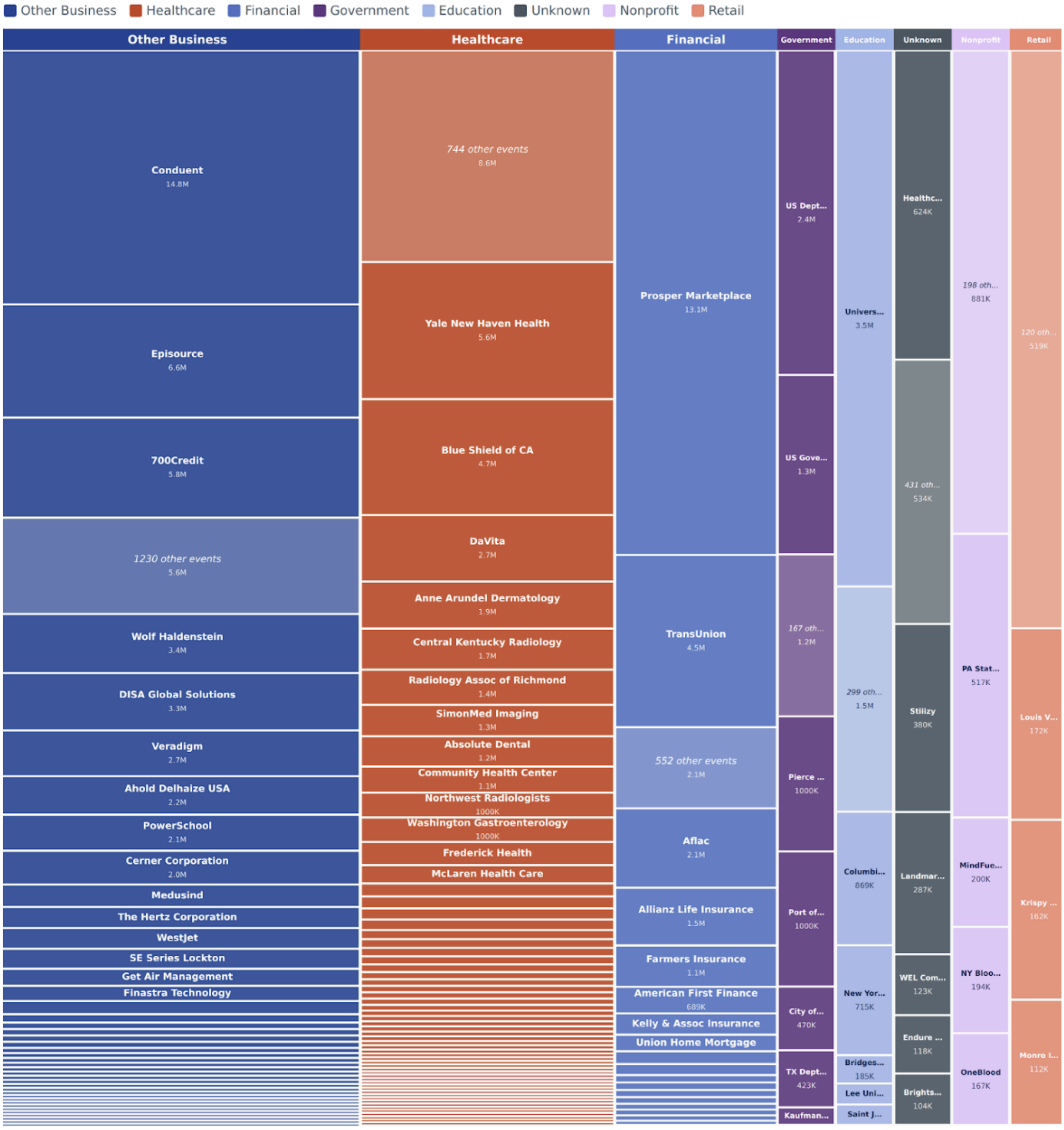


Figure 4. Area corresponds to individuals affected. All breaches of 100,000+ shown individually. Healthcare includes HIPAA covered entities. Other Business includes tech, manufacturers, utilities, legal services, data brokers.

V. THE BREACH METHOD TRANSPARENCY GAP

Understanding how breaches happen is essential to preventing them, but breach notifications and the agencies that publish them rarely provide that information with much specificity. The transparency gap operates at two levels.

First, many state attorneys general publish summary tables about breach filings rather than the actual notification letters sent to consumers. These tables typically list the organization name and when the breach was reported.They might include when the breach occurred, impact numbers, or a generic categorization like "hacking" or "unauthorized access." Even when impact numbers are provided, they're often limited to the number of individuals impacted in that state rather than the full scope of the breach. As discussed earlier, the PowerSchool breach illustrates this problem. Filings across multiple states reported state-specific counts, but no single notification disclosed the total number of students and educators affected nationwide. Massachusetts, Texas, Indiana, and Oregon together account for more than half of all 2025 notifications, and none provide the underlying letters where breach details would appear. For these 4,100+ filings, we have no information about how the breach occurred beyond surface-level labels.

Second, even among the 40% of notifications where we have access to actual breach notification letters, specificity remains rare. Of the 1,647 breach events with notification letters available, only 17% mentioned a specific attack method like ransomware, phishing, malware, or a software vulnerability. The rest describe incidents in generic terms: 80% mention "suspicious activity," 68% reference a "security incident," and 45% describe "unauthorized access" without explaining how attackers got in.

Where organizations disclose specifics, no single attack method dominates. Ransomware appeared in 111 notification letters. Phishing was mentioned in 105. References to software vulnerabilities appeared in 41, malware in 33, and social engineering in 15. These categories overlap considerably: a phishing email can deliver ransomware, stolen credentials can enable email compromise, and a single intrusion may involve multiple techniques. The 111 letters mentioning ransomware almost certainly undercount the actual prevalence, as many organizations describe only "encryption" of systems or "network disruption" without using the word ransomware.

The incidents that mention ransomware span every sector. Local governments proved particularly vulnerable: Union County in Pennsylvania (7,335 affected), Union County in Ohio (45,487), Mower County in Minnesota (27,064), and several others disclosed ransomware attacks in 2025. Schools faced similar pressures, including Madison Elementary School District 38 (35,000 affected) and Prince George County Public Schools (3,959). Healthcare organizations remained frequent targets: Wayne Memorial Hospital (163,440) and dozens of smaller practices explicitly mentioned ransomware. Law firms also appeared as a notable category, with Berman & Rabin disclosing an attack that encrypted files, affecting over 150,000 individuals. LaBovick Law Group, Daniels Law Group, and Shrader & Associates also reported ransomware incidents.

By the Numbers

Breach Method	Events	Affected
Unknown	2,032 (50%)	16.7M
Hacking/Malware	1,844 (45%)	351.1M
Unintended Disclosure	127 (3%)	5.6M
Physical/Portable Device	50 (1%)	158K
Insider Threat	21 (<1%)	1.4M
Payment Card Fraud / Card Skimming	3 (<1%)	25K

These tables reflect breach events, not raw notification counts. By consolidating filings across multiple states for the same incident, we can often piece together a more complete picture than any single state's disclosure provides. Even so, 50% of events remain categorized as "Unknown" method, while the 45% classified as hacking or malware account for 94% of all affected individuals. The attacks causing the most harm are precisely the ones where understanding the method of compromise could inform better defenses. Both stronger disclosure requirements in state notification laws and a commitment from reporting agencies to publish the underlying notification letters would help close this gap.

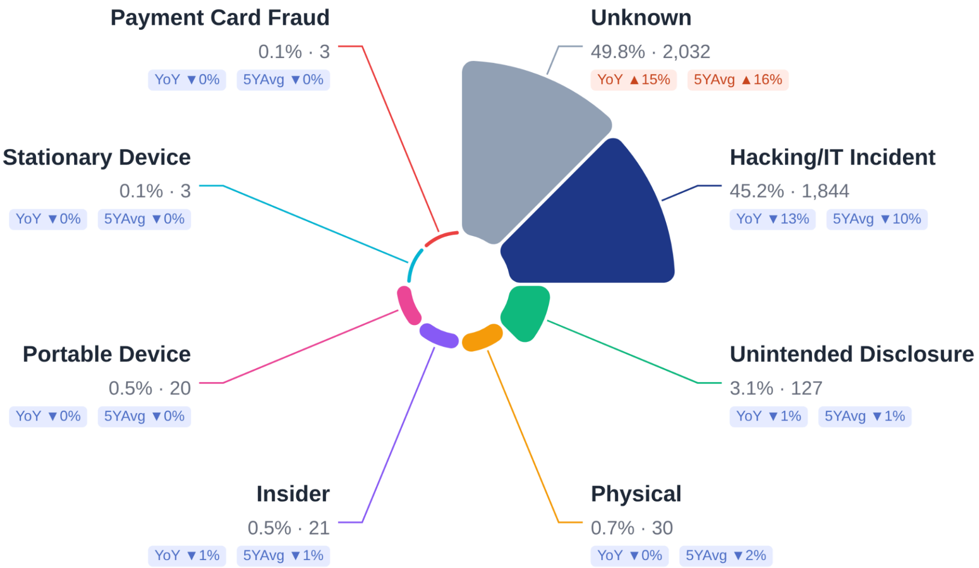


Figure 5. Unique breach events by method, with year-over-year and five-year average comparisons shown below each category. Nearly half of 2025 events have unknown methods (up 15% from last year) reflecting limited disclosure requirements in many states. Among events with known methods, hacking and malware account for 45% of events but 94% of affected individuals.

Organization Type	Events	Affected
Other Business (BSO)	1,338	76.2M (20%)
Healthcare (MED)	875	**249.3M (66%)**
Financial (BSF)	602	28.2M (8%)
Unknown (UNKN)	442	2.9M (<1%)
Education (EDU)	310	6.9M (2%)
Nonprofit (NGO)	207	2.0M (<1%)
Government (GOV)	180	8.1M (2%)
Retail (BSR)	126	1.3M (<1%)

Healthcare's domination in the affected count is almost entirely attributable to Change Healthcare. Remove that single breach, and healthcare would drop to roughly 56 million affected, behind the "Other Business" (BSO) category at 76.2 million. The BSO category captures the vendor and service provider ecosystem that processes data on behalf of other organizations, including companies like Conduent, Episource, and 700Credit that appeared in this year's largest breaches.

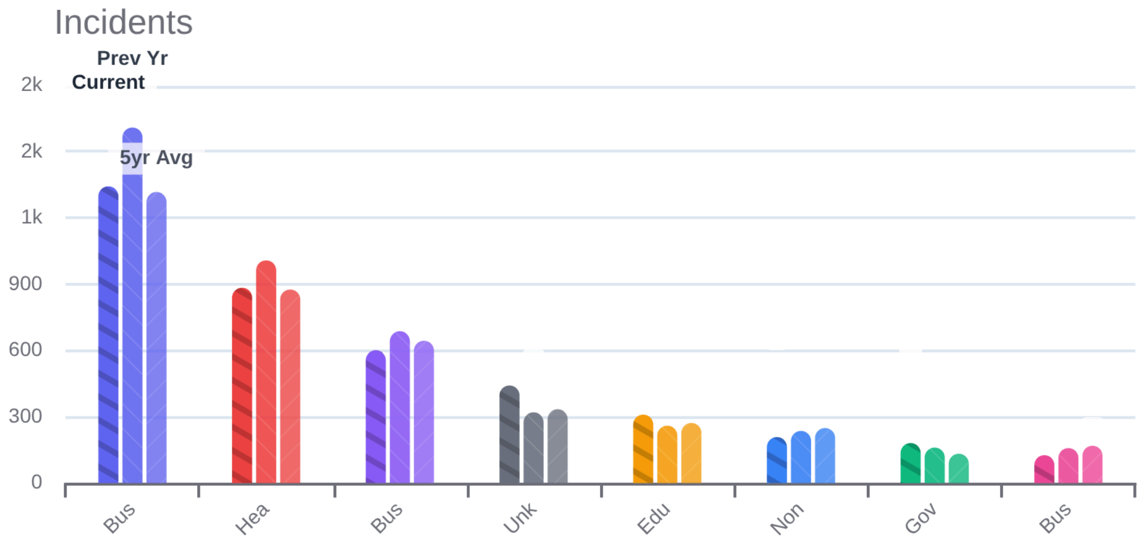


Figure 6. Breach events by organization type (left), compared to the previous year (middle) and five-year average (right). Business service providers lead in event count, though healthcare dominates in total individuals affected in 2025 due to the Change Healthcare continuing notifications from 2024. The "Unknown" category reflects filings where organization type could not be determined from available information.

VI. THE NOTIFICATION LAG PROBLEM

When did the breaches reported in 2025 actually occur? For thousands of breaches, we don't precisely know. 46% of breach events reported in 2025 have unknown breach dates. Of those with known dates, the timeline tells a story of delays between when a breach occurs and when consumers learn their information was compromised:

When Breach Occurred	Events Reported in 2025
2025	1,092 (27%)
2024 (second half)	830 (20%)
2024 (first half)	211 (5%)
2023	61 (1.5%)
Before 2023	14 (<1%)
Unknown breach date	*1,872 (46%)*

Only about a quarter of 2025's breach notifications involved incidents that actually occurred in 2025. The rest are catching up, some from late 2024, some from earlier. Change Healthcare's final notification of 2025, filed 20 months after the breach, is an extreme example but not an outlier in direction.

Looking at the 13,729 breach events from 2020-2025 where we have both breach and notification dates, the most common notification window is 91-180 days, accounting for 29% of all breaches. Nearly a quarter take six months to a year to reach consumers, and 7% take more than a year. Consumers whose information has been exposed remain unaware and unable to take protective steps while bad actors exploit stolen data.

California’s SB 446: A New Standard

This year, California enacted SB 446, establishing a 30-day deadline for breach notification (and a 15-day deadline for notification to the attorney general for breaches impacting more than 500 Californians), creating one of the strongest requirements in the nation. Privacy Rights Clearinghouse proudly supported this legislation alongside a coalition of privacy and civil liberties organizations.

Until SB 446, California law required notification "in the most expedient time possible and without unreasonable delay," a vague standard that left room for interpretation. Our data show the results of that ambiguity. Looking at California-reported breach notifications from 2020-2025, the average time to notify consumers was 192 days. The median was 136 days. It's difficult to see how those timelines squared with the statutory requirement for notification "in the most expedient time possible."

SB 446 gives that vague language a concrete meaning. The 15/30-day clock starts when a breach is discovered. Based on our 2020-2025 data, less than 4% of breaches nationally resulted in notification within 15 days, and only 10% of breaches nationally would meet the 30-day deadline. We'll be watching closely to see how that changes as the new law takes effect.

Time from Breach to Notification (2020-2025)

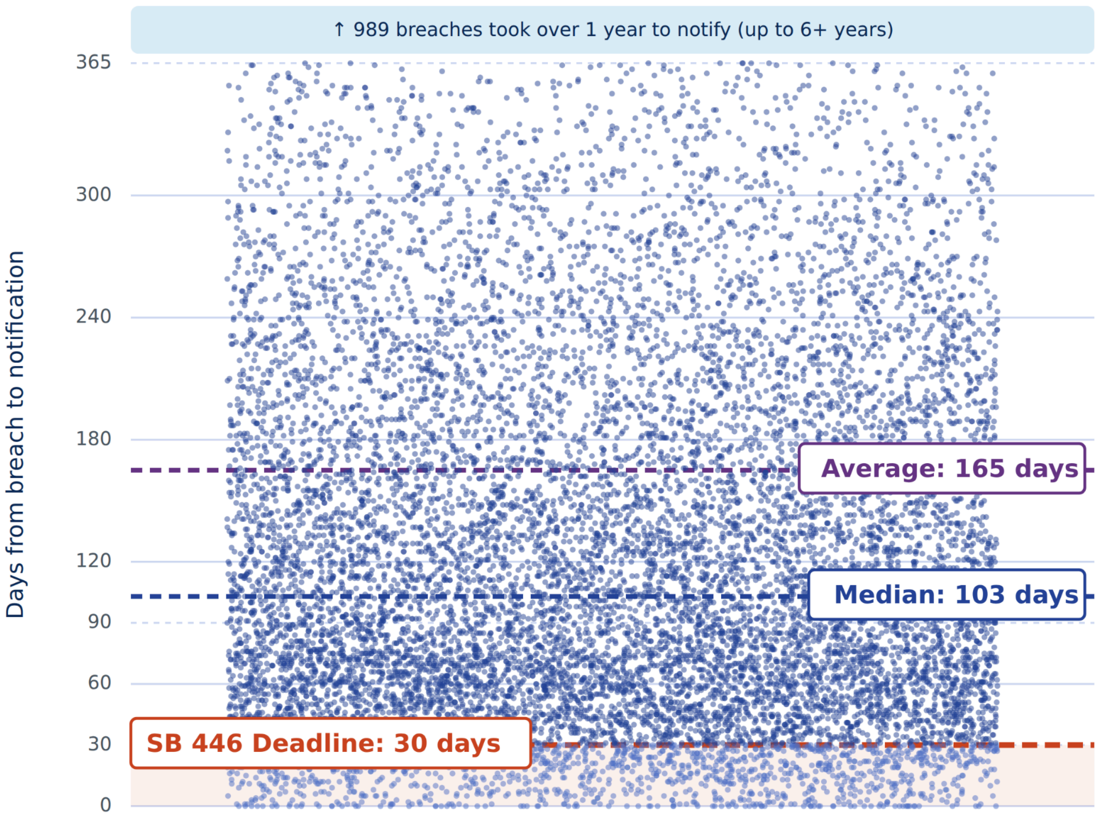


Figure 7. Each dot represents a breach event. Only 3.7% of breaches reported since 2020 with both breach date and reported date available for analysis would meet California's new SB 446 15-day notification deadline, and only 10% of breaches had notifications sent out within 30 days. The typical breach takes 3-4 months to reach consumers.

VII. WHAT 2025 TELLS US

1. **Healthcare remains a consequential breach target.**
   The sector accounted for 66% of all affected individuals in 2025, driven by Change Healthcare but extending across hospital systems, radiology practices, dialysis providers, and dental groups. Healthcare data is uniquely sensitive. It can't be changed like a credit card number, victims are often in a vulnerable time of their life, and the sector's complex vendor relationships create a cascading risk of exposure.

2. **Vendor and supply chain risk dominates.**
   Some of the year's biggest breaches, including Change Healthcare, Conduent, and PowerSchool were all service providers whose compromise affected organizations and individuals several layers removed. In fact, eight of the twenty largest breaches reported in 2025 occurred at service providers, together accounting for 231 million of the year's 375 million affected individuals. Most of those 231 million people likely had no direct relationship with the company that exposed their data. Modern data supply chains mean that a breach at a company someone has never heard of can expose their most sensitive information.

3. **The credit data ecosystem concentrates risk in companies people don’t choose to engage with.**
   TransUnion's breach affected 4.5 million people, and one of the largest credit bureaus offering their own credit monitoring as a breach remedy underscores the problem, but credit data flows well beyond the big three bureaus. Data brokers like 700Credit resell credit reports to auto dealerships (5.8 million affected). Lending platforms like Prosper collect detailed financial information from applicants (13.1 million affected). These types of entities collect data on nearly every American adult, often without meaningful consent, and their security failures have outsized consequences.

4. **Notification timelines remain problematic.**
   With 46% of breaches lacking reported occurrence dates, consumers often can't know how long their data was exposed. Of breaches with known dates, the most common notification window is 91-180 days, and less than 10% would meet California's new 30-day standard under SB 446. Scale creates its own delays as well. Change Healthcare knew by July 2024 that 192.7 million people were affected, but notifications to individual victims continued through late 2025 as the company worked to identify who specifically was impacted and which healthcare entity's data was involved.

5. **Breach transparency remains inadequate.**

   In 2025, we captured only 13 of the 21 states that share breach notifications filed with their offices, and more than half of those we source notifications from publish only summary tables, not the actual notification letters where breach details would appear. Even among the 40% of events where we could access letters, only 17% mentioned a specific attack method like ransomware, phishing, or a software vulnerability. Equally opaque is often the true scope of major breaches. When incidents affect customers across multiple states, filings may report state-specific counts but frequently do not disclose the total number of individuals affected nationwide. These gaps make it harder for organizations to learn from each other's incidents, for policymakers to craft targeted regulations, and for consumers to make informed decisions about their own risk.

6. **Education faces growing risk.**

   The PowerSchool breach illustrates the transparency gap at its most extreme. While independent reporting suggests up to 62 million students and families may have been affected, state notification filings, each reporting only that state's residents, account for fewer than one million confirmed individuals. The true scope remains unknown. Columbia University, NYU, and dozens of school systems also reported significant incidents in 2025. Educational institutions and edtech vendors hold uniquely sensitive data about students, many of them minors, and this data will often follow these individuals for decades. Yet when edtech vendors are breached, a single compromised platform may expose students across thousands of institutions, with data ranging from grades and test scores to financial aid status and health information.