

WASHINGTON STATE ATTORNEY GENERAL'S

# 2025 DATA BREACH REPORT




ATG.WA.GOV





This is the 10th annual Data Breach Report published by the Attorney General's Office (AGO).<sup>1</sup> We provide this report as a service to Washingtonians, because we are best able to safeguard our data when we are aware of the threats.


A data breach is the unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by a person, business, or agency. Washington law requires private<sup>2</sup> and public<sup>3</sup> entities impacted by a data breach to notify Washingtonians whose personal information is compromised, as well as to notify the AGO if the breach impacts more than 500 Washingtonians. This report is based on data breach notifications received by the AGO between July 24, 2024, and July 23, 2025.<sup>4</sup>

## KEY TAKEAWAYS

 Over the past year, the Attorney General's Office has been notified of 209 separate data breach incidents impacting just over 8 million Washingtonians.

 This is the second straight year that the number of notices sent to Washingtonians has exceeded the state's population (approximately eight million residents), suggesting that millions of Washingtonians experienced multiple breaches of their personal information within a single calendar year, yet again.

 Cyberattacks, particularly ransomware attacks,<sup>5</sup> were again the most common type of breaches.



 The impact and scope of these data breaches are staggering, and there is more that the state, entities, and individuals can do to prevent Washingtonians' personal information from being compromised.



## RECOMMENDATIONS

To provide consumers with more transparency and control over how and where their data is collected, stored, and shared, the AGO recommends that policymakers:

1. Make improvements to the state's data breach notification law by:

-  Creating language access requirements for data breach notifications that allow all Washingtonians the opportunity to receive notice in their native language improving the likelihood that our state's Limited English Proficiency communities will receive the information they need to protect themselves and their data; and
-  Expanding the definition of "personal information" in RCW 19.255.005 to include (a) Individual Tax Identification Numbers (ITINs) and (b) full name in combination with a redacted Social Security Number (SSN) that still exposes the last four digits of the number.



2. Require businesses to recognize and honor opt-out preference signals and give Washingtonians more control over how their data is collected and used;
3. The Legislature should pass HB 1887, creating a data broker registry for Washington State which would provide much needed transparency to consumers and agencies about the location and sale of Washingtonians' data. <sup>6</sup>
4. The AGO should leverage its outreach to consumers through surveys and stakeholder engagement to understand their concerns around data breaches and data privacy and use these findings to:

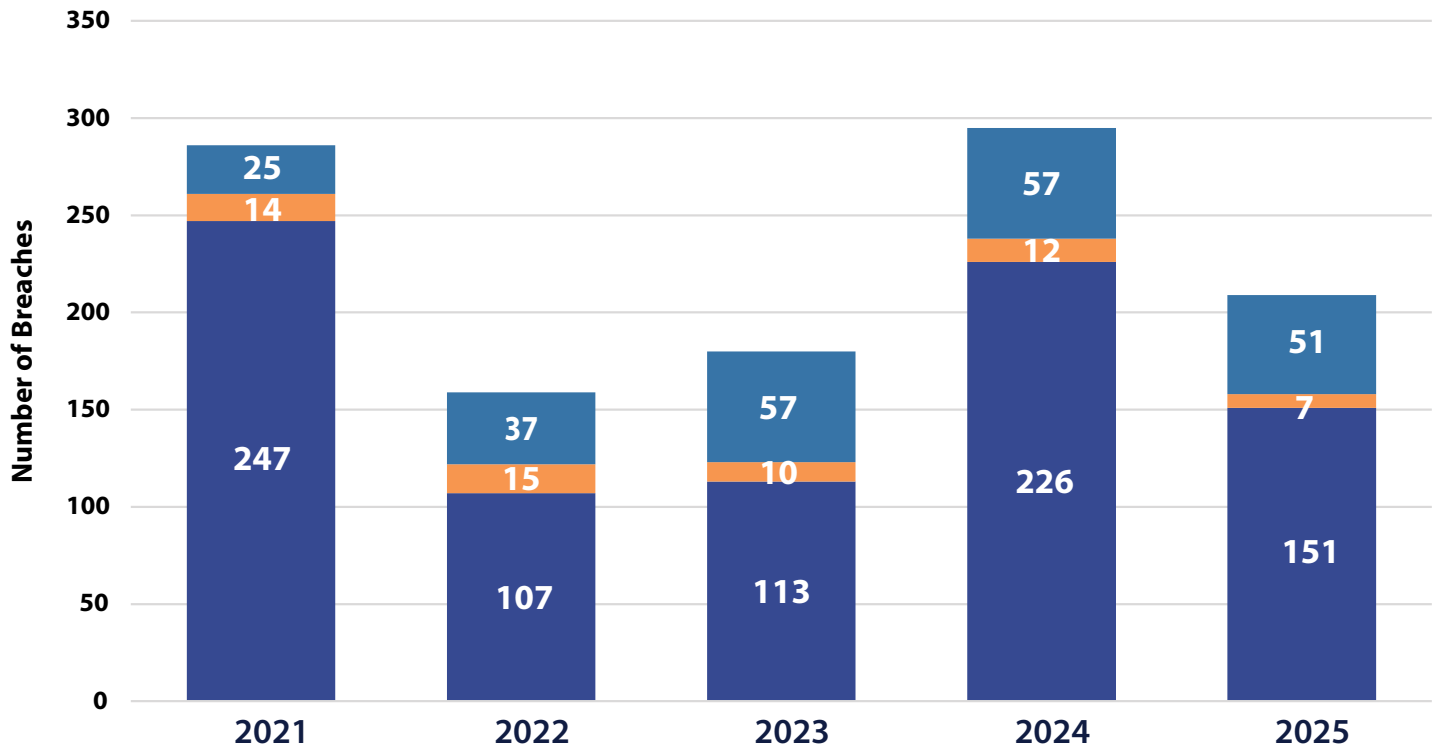
-  Generate additional data privacy resources and tools for the public; and
-  Develop recommendations to address gaps in data privacy policy that can lead to data breaches.



For more details on these recommendations, please refer to the "Recommendations" section in the 2024 Data Breach Report, available online at <https://www.atg.wa.gov/data-breach-reports>.

## Total Number of Data Breaches by Cause

■ Cyberattack ■ Theft or mistake ■ Unauthorized access

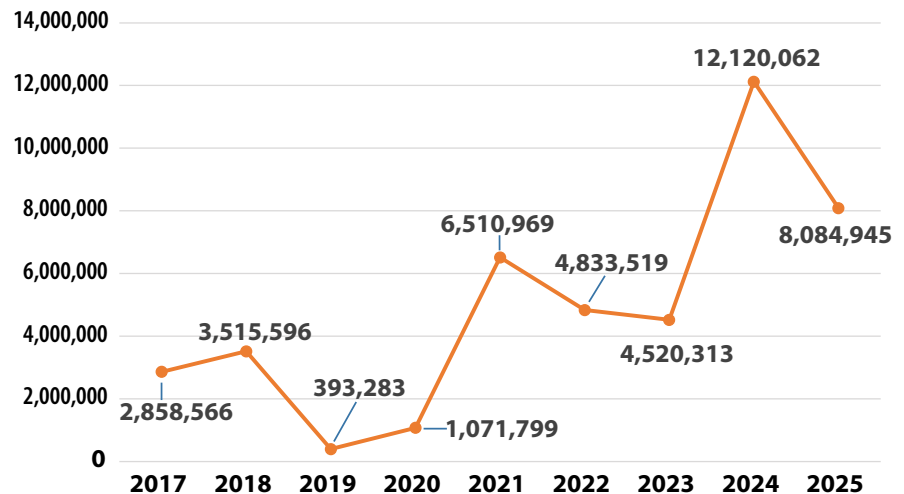


### Data breaches fall into three broad categories:

- 1. Cyberattack:** A third party deliberately attempts to access secured data, such as information stored on a server, using cyber technology. The attack can use a skimmer, spyware, phishing email, ransomware, or similar means of accessing secure data remotely.<sup>7</sup>
- 2. Theft or mistake:** The mistaken loss of information, such as a clerical error that sent W-2 information to an unintended recipient, or the inadvertent theft of information, such as stealing a laptop that happened to contain patient medical records.
- 3. Unauthorized access:** An unauthorized person purposefully accesses secure data through means such as an unsecured network or sifting through sensitive documents left out on a desk.

## NUMBER OF WASHINGTONIANS AFFECTED BY DATA BREACHES

In 2025, 209 data breaches that affected more than 500 Washingtonians' personal information were reported to the AGO.



### Top Five Largest Breaches Affecting Washington Residents in 2025

Breached Entity	Industry	Date Reported to AGO	Washingtonians Affected
Change Healthcare Inc.	Health	8/03/2024	3,121,209
QuoteWizard	Business	8/05/2024	717,781
Washington Gastroenterology	Health	5/23/2024	556,349
Laboratory Services Cooperative	Non-Profit/Charity	4/10/2025	465,487
Northwest Radiologists Inc./Mount Baker Imaging	Health	7/10/2025	348,118

## KEY STATISTICS

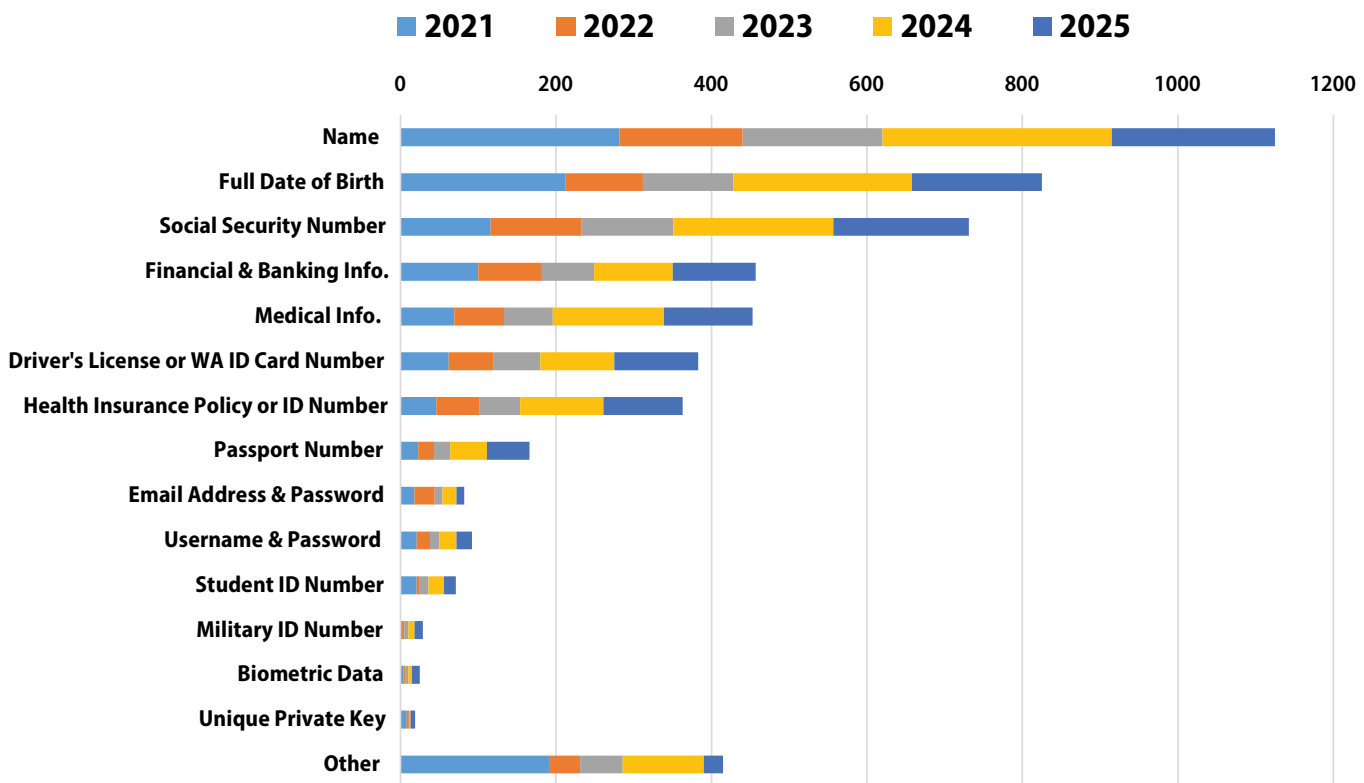
Although the overall number of reported breaches is lower than 2024, it still represents the third highest total recorded in Washington at 209 breaches.

The number of breaches impacting more than 50,000 Washingtonians is in double digits for the fifth straight year, and for the second straight year has reached at least 20 such breaches in a single year.

The overall number of Washingtonians affected in 2025 represents the second highest total recorded in Washington and includes yet another mega breach affecting 1 million or more Washingtonians (Change Healthcare Inc. – 3.1 million).

The Change Healthcare Inc. data breach was the result of a ransomware attack. Ransomware attacks were the most common method of cyberattack reported in 2025 (65%). The healthcare industry is particularly susceptible to ransomware attacks, as they hold highly sensitive and timely patient data. Being locked out from this information could put patients at risk of physical harm, and thus healthcare entities are more likely to meet the demands of a ransomware attack to protect their patients. Over the last five years (2021-25), the healthcare industry has reported 87 breaches caused by ransomware, second only to business (177).

## TYPES OF PERSONAL INFORMATION COMPROMISED



In 2025, 173 breaches, representing just over 80% of all breaches reported, resulted in the compromise of Washingtonians' Social Security numbers (SSN). SSNs have been among the top three compromised pieces of personal information in every report since 2016. This is likely due to how valuable SSNs are to hackers and would-be identity thieves, as they are often required for individuals to access financial products, such as applying for a loan, and government services and benefits, like Medicare.

**Over 80% of breaches compromised SSNs**



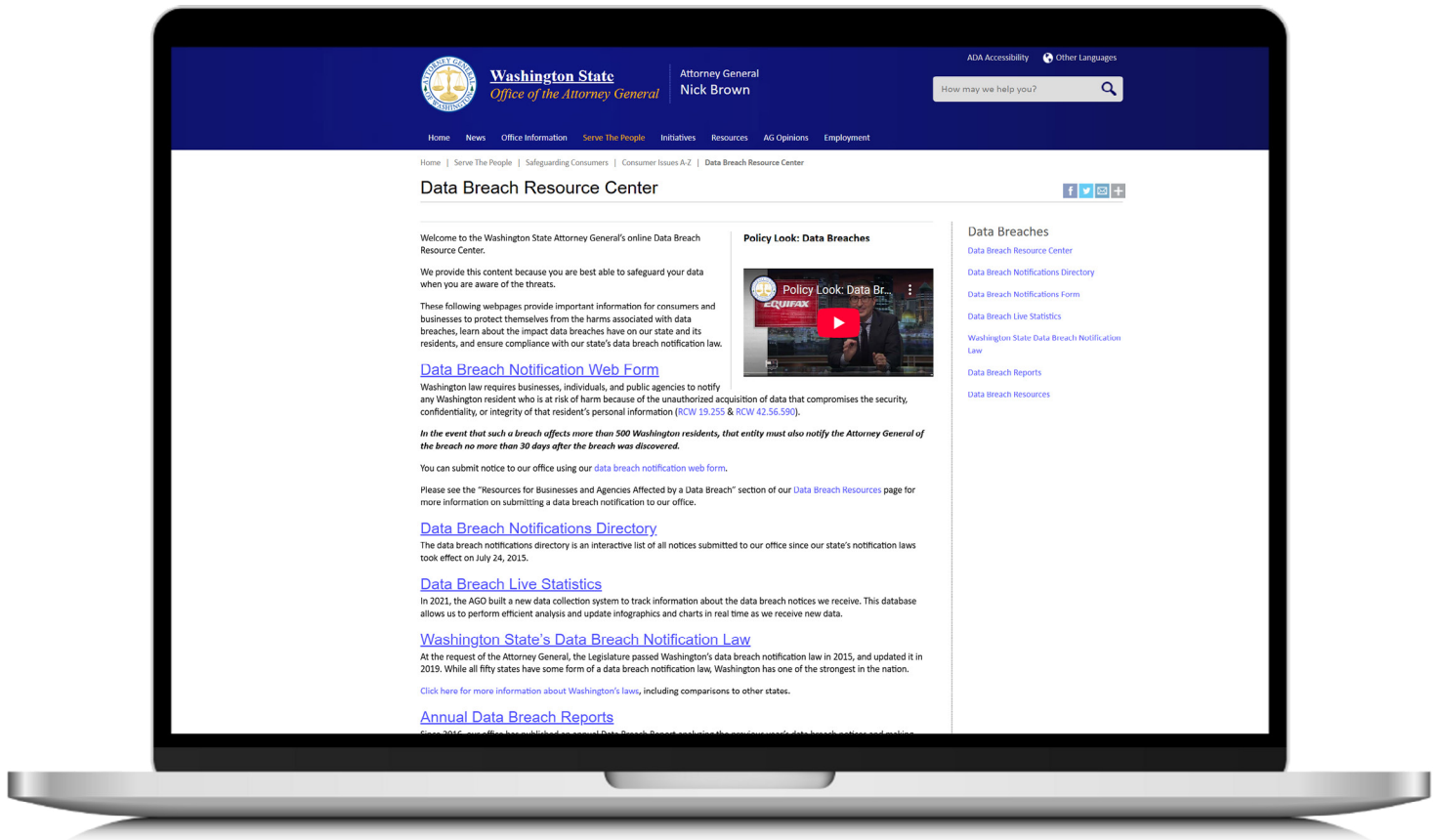
Overall, full date of birth (167 breaches) was the second most compromised piece of personal information in 2025. Date of birth is often required in validating an individual's identity for several services and products. While on the surface, a full date of birth may not seem like the most sensitive piece of information, in combination with any of the other categories above – such as SSNs – the acquisition of a full date of birth could be of great consequence, and a windfall for identity thieves.

## ADDITIONAL AGO ACTIONS

In January 2025, the Attorney General's Office filed a lawsuit against T-Mobile for failing to adequately secure the sensitive personal information of more than 2 million Washingtonians.<sup>8</sup> That failure resulted in a massive 2021 data breach that exposed the personal information of those consumers and made them vulnerable to fraud and identity theft. T-Mobile then compounded the harm by sending those consumers deceptive and legally inadequate data breach notifications. Meanwhile, despite these failures, T-Mobile had publicly assured consumers that it implemented robust safeguards to protect their personal data. As part of the lawsuit, the Attorney General will seek injunctive relief to require improvements to T-Mobile's cybersecurity policies and procedures, as well as increased transparency in communications about cybersecurity, and compliance with Washington's data breach notification law. The lawsuit is currently pending in King County Superior Court.

Thank you for reading the Washington State Attorney General's Office 2025 Data Breach Report.

If you are interested in additional information and resources for both consumers and businesses, please consider visiting our office's online Data Breach Resource Center at: <https://www.atg.wa.gov/data-breach-resource-center>.



This webpage contains past reports, live updating data breach statistics, published copies of data breach notices received by our office, information about our state's data breach notification laws, and more.

If you would like to file a consumer complaint with regards to a data privacy incident, please visit our online complaint form available at [www.atg.wa.gov/file-complaint](http://www.atg.wa.gov/file-complaint) or call the Consumer Resource Center at 1-800-551-4636.

## Notes and Citations

<sup>1</sup> Previous Data Breach Reports can be found online at: <https://www.atg.wa.gov/data-breach-reports>

<sup>2</sup> See, [RCW 19.255](#).

<sup>3</sup> See, [RCW 42.56.590](#).

<sup>4</sup> Additional information on our data gathering and analysis process can be found online at: <https://www.atg.wa.gov/data-breach-live-statistics>.

<sup>5</sup> A ransomware attack is a type of malicious software that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. See our "Glossary of Data Breach Terms" for definitions of the various forms of cyberattacks that exist, here: <https://www.atg.wa.gov/glossary-data-breach-terms>.

<sup>6</sup> HB 1887 – 2025-26, <https://app.leg.wa.gov/billsummary?BillNumber=1887&Year=2025>

<sup>7</sup> See our "Glossary of Data Breach Terms" for definitions of the various forms of cyberattacks that exist, here: <https://www.atg.wa.gov/glossary-data-breach-terms>.

<sup>8</sup> See press release, January 6, 2025, available here: [AG Ferguson files lawsuit against T-Mobile for massive data breach | Washington State](#).

