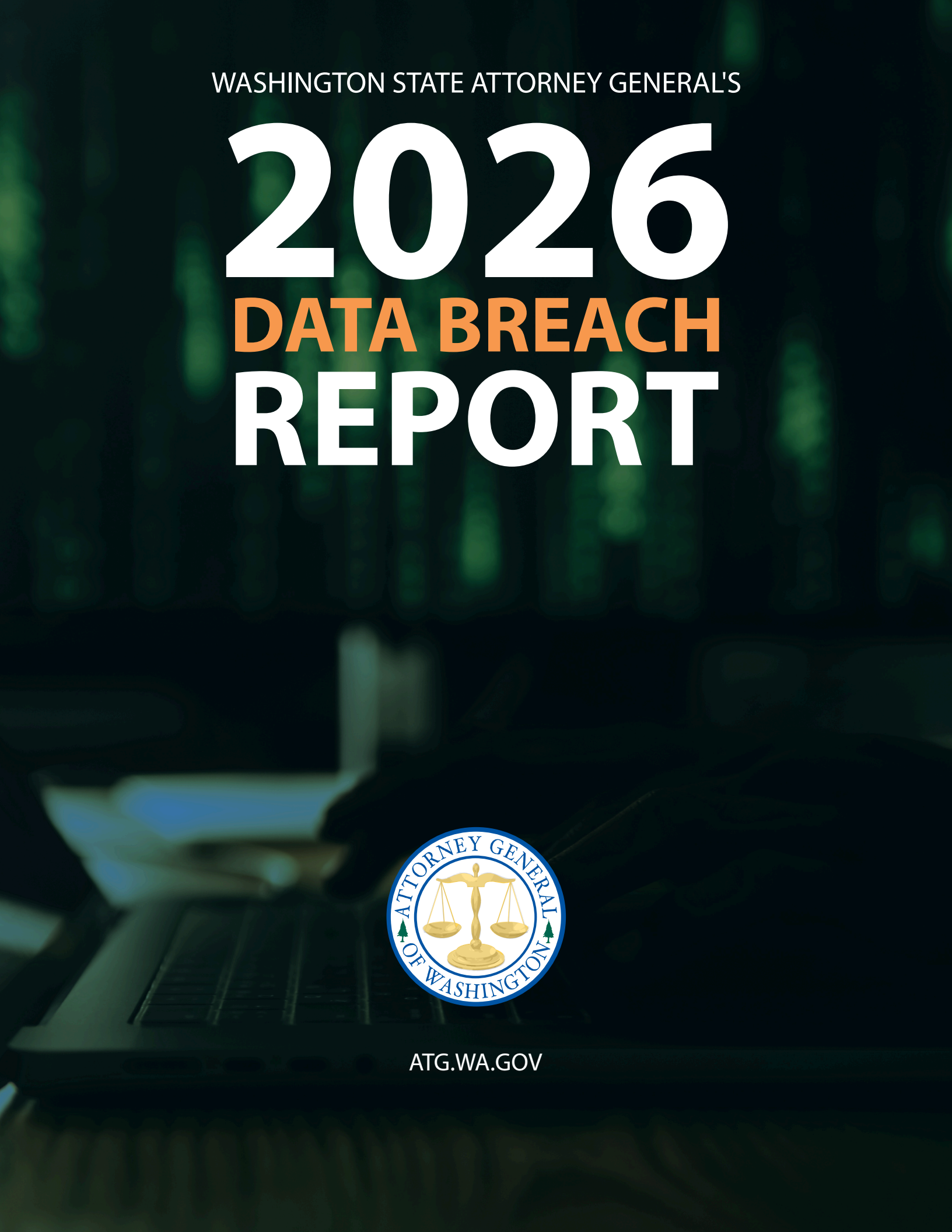
WASHINGTON STATE ATTORNEY GENERAL'S

# 2026 DATA BREACH REPORT



ATG.WA.GOV

## LETTER FROM THE ATTORNEY GENERAL

Dear Washingtonians,

For more than a decade, our office has issued annual reports that track data breaches affecting Washington residents. We do so to better understand the scope of these incidents, identify the causes, and find opportunities to strengthen protections for Washingtonians. For that reason, I am pleased to present this year's Washington State Attorney General's annual Data Breach Report.

Every day, Washingtonians entrust businesses, government agencies, and other institutions with personal information. We expect these institutions to keep our information safe and to use it responsibly. Data breaches continue to put sensitive information at risk, exposing residents to identity theft, financial fraud, and other types of lasting harm for individuals and families. Cybercriminals continue to develop new methods of accessing sensitive information, from increasingly sophisticated ransomware attacks to scams and other cyberattacks enabled by generative artificial intelligence. As these threats evolve, so must our approach to protecting personal information.

Washington has taken important steps to protect residents' personal information. But, as noted in our office's recent Data Privacy Report, Washingtonians remain concerned about how their information is collected, stored, and shared. They want greater transparency and control over personal data. They also deserve to be notified promptly when that information is compromised.

This year's report builds on our office's longstanding efforts to document data breaches, inform the public, and find gaps in existing protections. It also offers recommendations to strengthen Washington's data breach notification laws and ensure residents receive the information they need to protect themselves when their personal data is exposed.

Protecting Washingtonians' personal information is an ongoing responsibility shared by government, businesses, and other institutions that collect and maintain sensitive data. I encourage policymakers and other stakeholders to use this report to strengthen accountability, improve data security, and build a safer digital environment for everyone in Washington.

Sincerely,



Nick Brown

Attorney General

## EXECUTIVE SUMMARY

This is the 11th annual Data Breach Report published by the Attorney General's Office (AGO).

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 held by a person, business, or agency.



Washington law requires private and public entities (data collectors) affected by a data breach to let Washingtonians know that their personal information is compromised. These laws were the result of legislation requested by the Attorney General motivated by several massive data breaches in the early 2010s.

In 2015, the Legislature passed legislation requested by the Attorney General requiring data collectors to provide notice to Washingtonians within 45 days of the discovery of a data breach, and to the AGO when a breach affects more than 500 residents. The Legislature amended the law in 2019, at the request of the Attorney General, reducing the deadline to notify residents to 30 days and greatly expanded the list of data types that trigger a notice. The first annual AGO Data Breach Report came out of the passage of the 2015 law and serves as a public resource tracking the impact of data breaches on Washingtonians.

This report is based on data breach notifications received by the AGO between July 24, 2025, and July 23, 2026. More information on our data gathering and analysis process can be found online at: atg.wa.gov/data-breach-live-statistics.

Previous Data Breach Reports can be found online at: atg.wa.gov/data-breach-reports.

## KEY TAKEAWAYS

- Over the past year, the AGO has been notified of 197 separate data breach incidents affecting more than 3.5 million Washingtonians. This is down from 2024 and 2025, and below our state's ten-year average (approximately 4.8 million notices per year).
- Cyberattacks, particularly ransomware attacks, were again the most common cause of data breaches.





### What is Ransomware?

Ransomware 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.

*Interested in learning more common data breach terms? Visit our online data breach glossary at [atg.wa.gov/glossary-data-breach-terms](atg.wa.gov/glossary-data-breach-terms)*

- No mega breaches affecting 1,000,000 or more Washingtonians were reported in 2026. This is the first full year without a mega breach affecting Washingtonians since 2023.
- Just over 75% of all data breaches reported in 2026 resulted in the exposure of a Washingtonian's Social Security number (SSN). SSNs continue to be one of the most consistently targeted data types exposed in breaches.
- Overall, data breaches continue to be a significant threat to the privacy of Washingtonians.

## RECOMMENDATIONS

Our state's data breach notification laws were last updated by the Legislature in 2019. In the seven years since those amendments, the data economy and the threats posed to Washingtonians' data have evolved significantly, from the rapid rise in ransomware attacks to advances in generative AI allowing cybercriminals to perform more sophisticated cyberattacks.

To meet these evolving threats and the needs of consumers, our office recommends legislators make the following changes to our existing data privacy laws, RCW 19.255 (governing data breaches of businesses) and RCW 42.56.590 (governing data breaches of public agencies):

1. Expand the definition of personal information in RCW 19.255.005(2)(a)(i) and RCW 42.56.590(10)(a)(i) to include the following data elements:

    a. Individual Taxpayer Identification Number (ITIN)

    b. Tribal Identification and Enrollment Numbers

    c. IRS Identity Protection PIN

    d. Precise Geolocation data (within 1,750 feet)

    e. Last four digits of a Social Security Number (already present in RCW 42.56.590)



2. Enhance protections for Washingtonians' personal information by adding language to RCW 19.255 requiring entities that own, license, or maintain data to implement and maintain reasonable security procedures and practices, appropriate to the nature of the information. Amendments should protect Washingtonians' personal information from unauthorized access, destruction, use, modification or disclosure. These might include:

    a. **Administrative safeguards** such as appointing one or more employees to coordinate a security program;

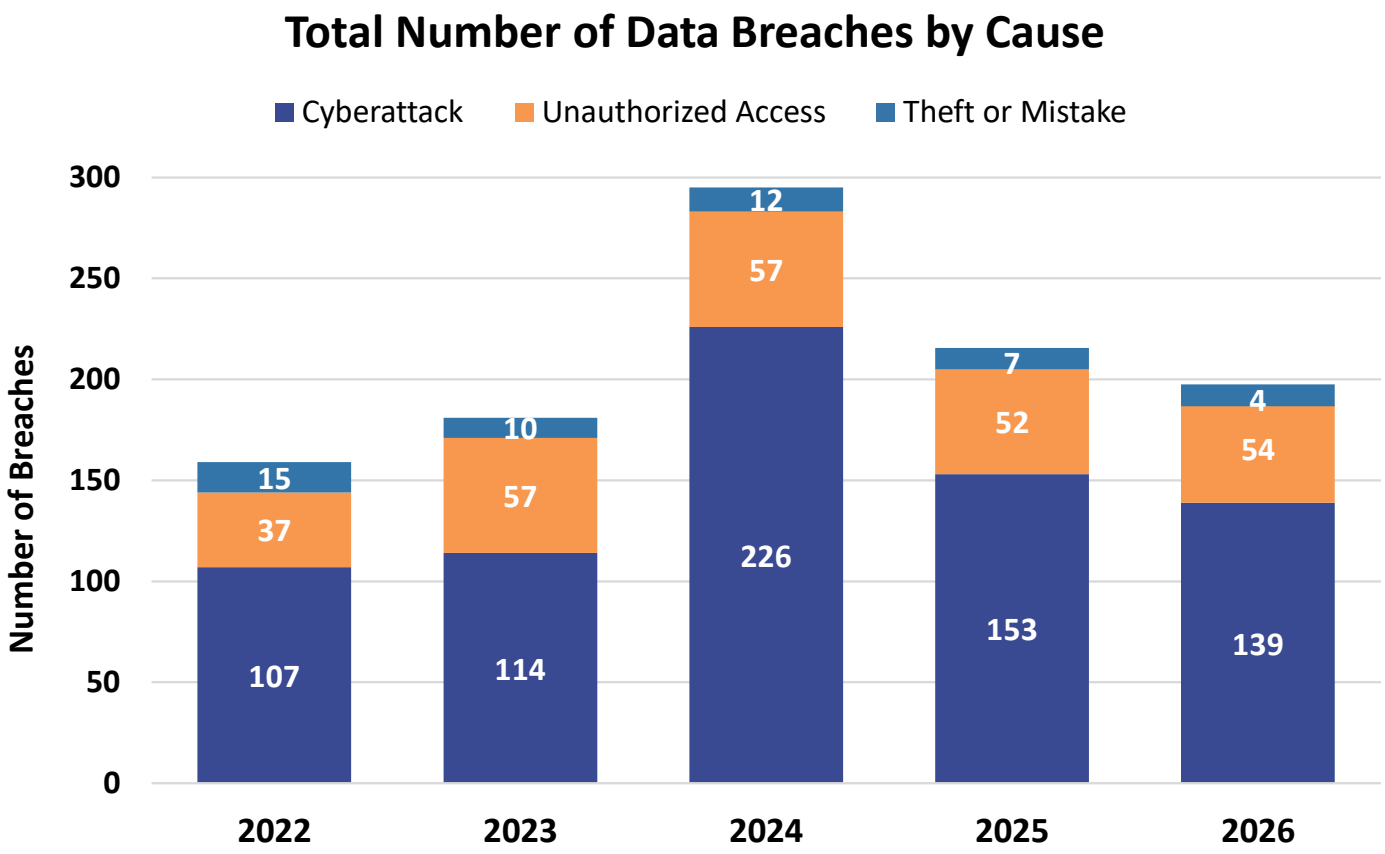
    b. **Technical safeguards** such as applying security updates to software that might reasonably be at risk of a data breach; and

    c. **Physical safeguards** such as disposing of personal information after the entity no longer needs the data for business purposes or as required by local, state or federal law.

3. Require notice by any entity in the event that an AI agent operated by the entity gains unauthorized access to a Washingtonian's personal information or a State Agency by amending RCW 19.255 and RCW 42.56.590.

Legislators should also consider supplementing the data breach notification law with additional legislation: (a) establishing a data broker registry; (b) imposing limits on the collection, sharing, and sale of biometric and precise geolocation data; and (c) establishing data minimization requirements and limits on secondary use. For more information on these broader data privacy proposals, please review the recommendations section of our office's 2026 Data Privacy Report.






Data breaches fall into three broad categories:

1. **Cyberattack**: A third party deliberately tries 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.

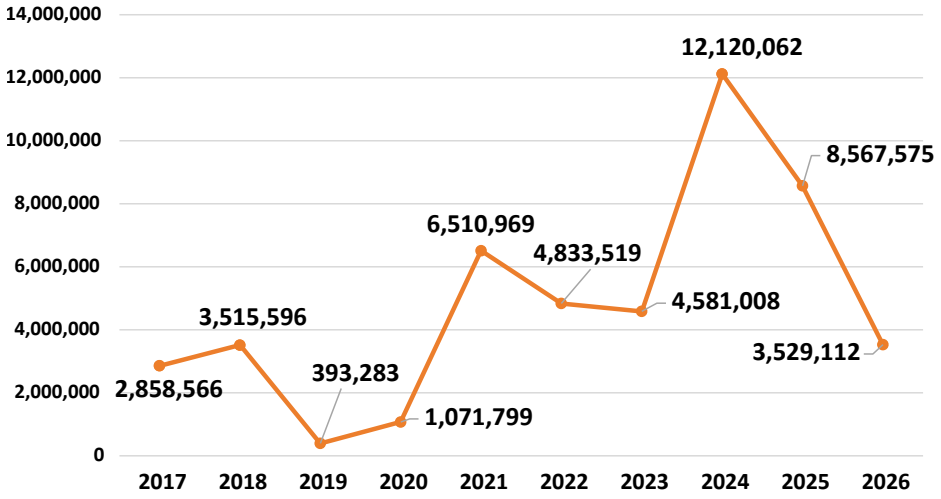
2. **Theft or mistake**: The mistaken loss of information, such as a clerical error that sent W-2 information to an unintended recipient, or the inadvertent theft of information, such as stealing a laptop that happened to contain patient medical records.

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.

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

## NUMBER OF WASHINGTONIANS AFFECTED

Data collectors must notify the Attorney General's Office of any data breaches that affect more than 500 Washington residents. Between July 24, 2025, and July 23, 2026, data collectors notified our office of **197** such incidents, resulting in a total of **3,529,112** notices sent to Washingtonians.



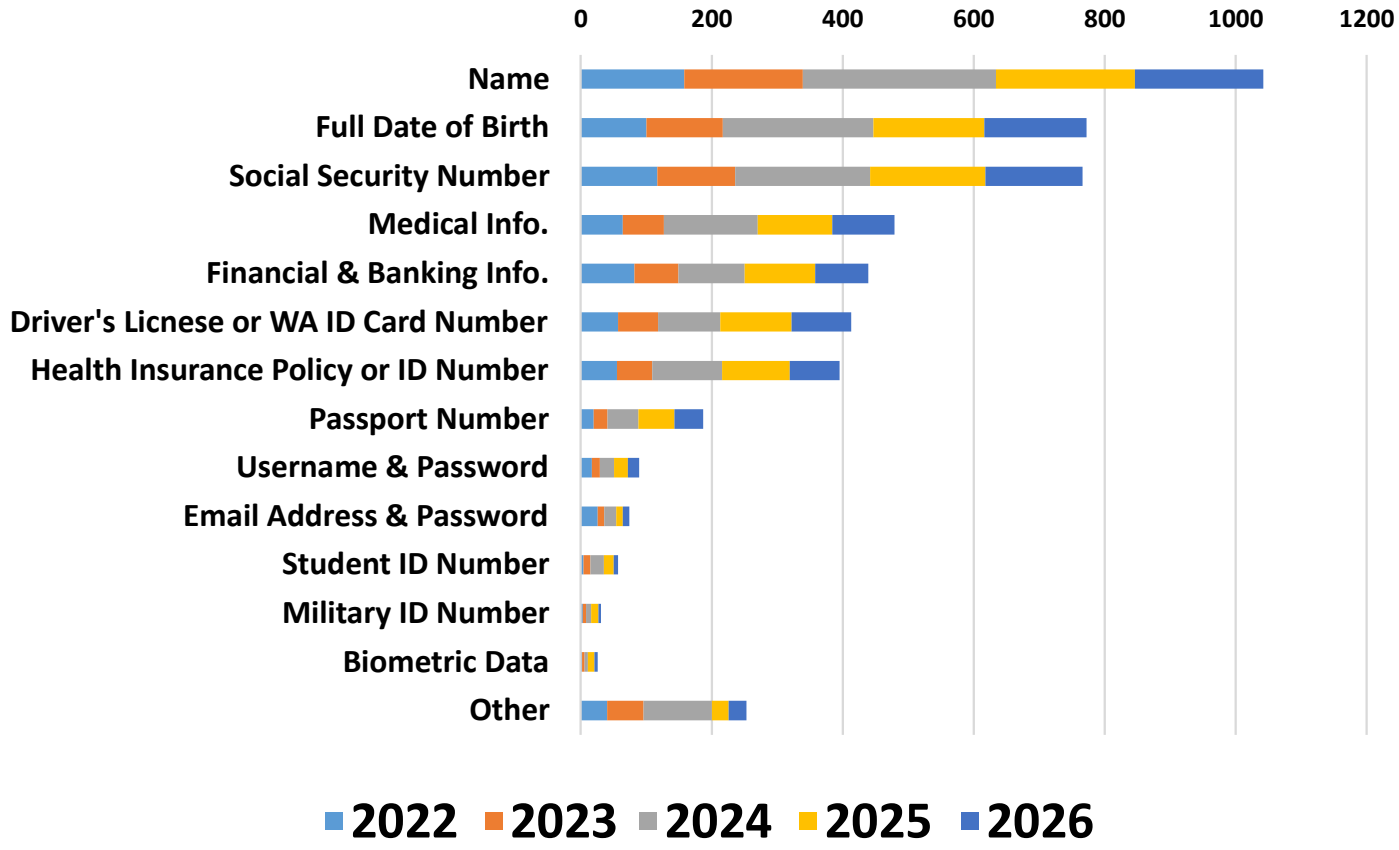

**Top Five Largest Breaches Affecting Washington Residents (July 24, 2025 – July 23, 2026)**

| Breached Entity | Industry | Date Reported to AGO | Washingtonians Affected |
|---|---|---|---|
| Conduent Business Services LLC | Business | 10/24/2025 | 786,927 |
| Navia Benefit Solutions, Inc. | Business | 3/18/2026 | 319,208 |
| Marquis Software Solutions | Business | 11/26/2025 | 269,773 |
| Prosper Marketplace, Inc | Finance | 12/9/2025 | 249,848 |
| DentaQuest, LLC | Health | 7/16/2026 | 148,300 |

***Key Statistics***

- The total number of reported breaches (197) decreased slightly from 2025 (212) but still represents the fourth highest total recorded in Washington since 2016.
- The number of breaches affecting more than 50,000 Washingtonians (14) is in the double digits for the sixth straight year.
- The overall number of Washingtonians affected in 2026 (3,529,112) represents the sixth highest total recorded in Washington since 2016.
- No mega breaches affecting 1 million or more Washingtonians were reported in 2026. The last time Washington went a full year without a reported mega breach was 2023.
- For the sixth straight year, ransomware was the most common method of cyberattack (85 incidents, 61% of all reported cyberattacks in 2026).

## Personal Information Exposed by Data Breaches



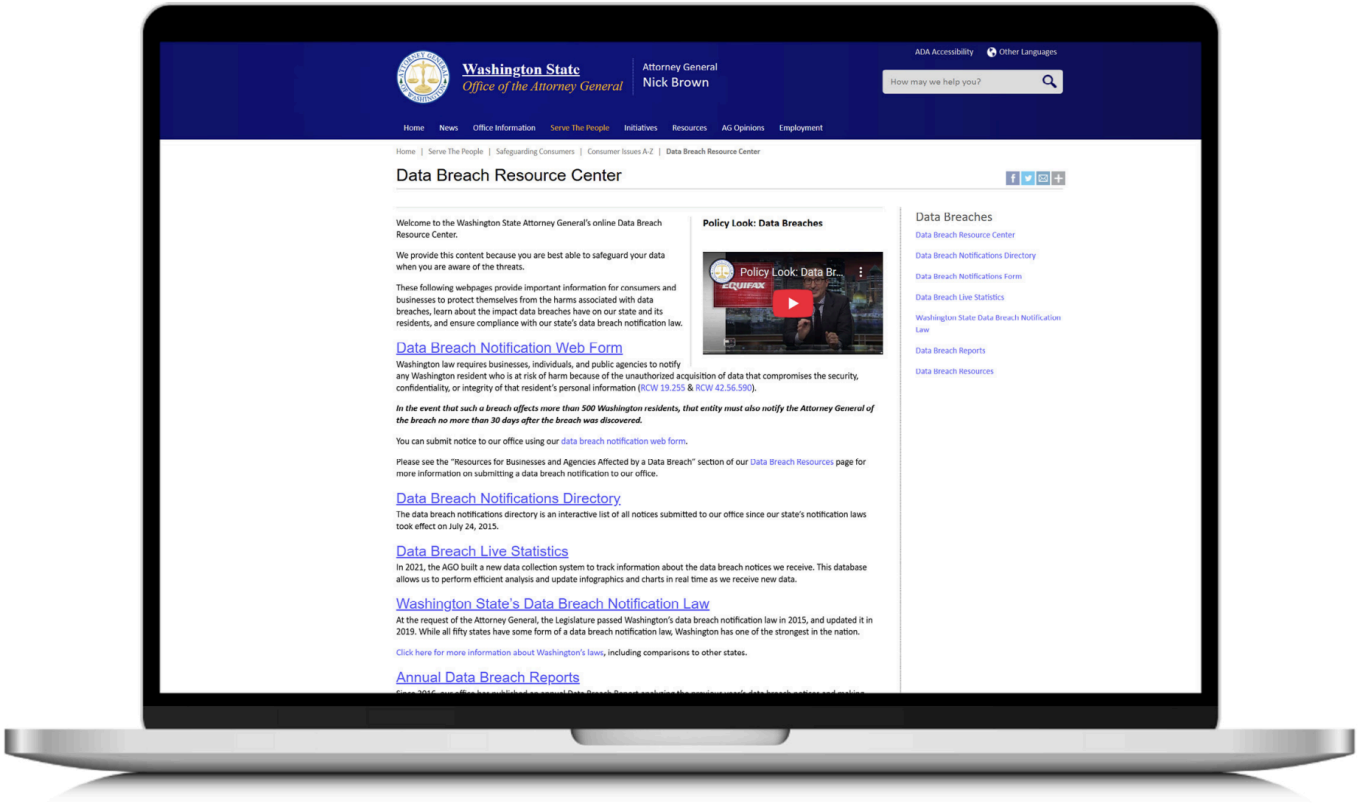

In 2026, 148 breaches, representing just over 75% of all breaches reported, resulted in the compromise of Washingtonians' Social Security numbers (SSN). SSNs have been among the top three compromised pieces of personal information in every report since 2016. This is likely due to how valuable SSNs are for identity theft, as they are often required for individuals to access financial products – such as applying for a loan – and government services and benefits, like Medicare.

Overall, full date of birth (156 breaches) was the most compromised piece of personal information in 2026. Date of birth is often needed to validate 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 categories above – such as SSNs – the acquisition of a full date of birth could be of great consequence, and a windfall for identity thieves.

## DATA BREACH RESOURCE CENTER

Thank you for reading the Washington State Attorney General's 2026 Data Breach Report.

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




This webpage contains past reports, live updating breach statistics, published copies of data breach notices receive 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 atg.wa.gov/file-complaint or call the Consumer Resource Center at 1-800-551-4636.