# WASHINGTON STATE ATTORNEY GENERAL'S OFFICE

# 2023

## DATA BREACH REPORT

# LETTER FROM THE ATTORNEY GENERAL

October 2023

Dear Washingtonians,

This is the eighth annual Data Breach Report published by my office. We provide this report as a service to Washingtonians, because you are best able to safeguard your data when you are aware of the threats.

Data breaches continue to be a significant threat to Washington residents, businesses, and agencies. In the last year, 133 data breaches were reported to our office, resulting in just over 4 million data breach notices sent to Washingtonians. This represents the third largest number of Washingtonians affected in a single year since we began tracking this data.

Additionally, ransomware attacks - a type of cyberattack that uses malicious code to hold data hostage in exchange for a ransom payment - continues to be the primary cause of these incidents. Ransomware attacks are particularly dangerous because they not only compromise consumers' privacy, but can impede critical services, such as healthcare or utility services, from being delivered to Washingtonians.

In 2023, 49 ransomware attacks were reported to our office, the second highest single year total since we began tracking this data. Ransomware attacks this year included 12 on healthcare facilities, and three on government institutions.

Consumers should have more control over how and where their data is collected, and more transparency about where their data is already stored. This report includes recommendations to provide consumers this control, including improvements to Washington's data breach notice laws, requirements for opt-out signal compliance, and regulations for data brokers.

My office also continues to initiate Consumer Protection Act cases against companies who experience data breaches because of lax data security that falls short of industry standards. These cases forced many companies to improve their security, and to date, my office has recovered approximately $17 million.

We will continue to enforce the law, and to provide Washingtonians the information needed to protect your business and your data.

Sincerely,

Bob Ferguson
Washington State Attorney General

# Executive Summary

- 2023 represents the third highest total number of data breach notices sent to Washingtonians (4 million) since 2016.
    - This is slightly down from 2022 (4.8 million). The all-time record is 6.5 million in 2021.

- The Attorney General's Office (AGO) received 133 data breach notifications in 2023 - also the third highest recorded amount since 2016.
    - This is also slightly down from 2022 (150). The all-time record is 285 notices in 2021. However, this is still more than double the 2017-2020 average of 66 notices per year.

- Cyberattacks, particularly ransomware attacks, were again the most common type of breaches.
    - Cyberattacks caused 61% of all reported breaches, compared to 86% in 2021 and 67% in 2022.
    - 49 breaches were caused by ransomware attacks. This is up from 2022 (46), and nearly five times the total number of ransomware breaches reported between 2017 and 2020 (10).
    - Ransomware attacks accounted for 61% of all cyberattacks (49 of 81) and just over a third of all breaches (37%).

## Background

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 entities impacted by a data breach to notify Washingtonians whose personal information is compromised, as well as to notify the AGO if more than 500 Washingtonians are impacted by the breach.

In 2019, Attorney General Ferguson proposed, and the Legislature passed, a bill strengthening Washington's data breach notification law. This legislation significantly expanded the definition of personal information, required notices to consumers to include the period of time their data was at risk, and reduced the deadline to provide notice to consumers to 30 days after the discovery of a breach. These changes went into effect on March 1, 2020.

This report is based on data breach notifications received by the AGO between July 24, 2022 and July 23, 2023 that affected more than 500 Washingtonians' personal information. Additional information on our data gathering and analysis process can be found on page 12.

## Recommendations

In order 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. Require businesses to recognize and honor opt-out preference signals and give Washingtonians more control over how their data is collected and used;

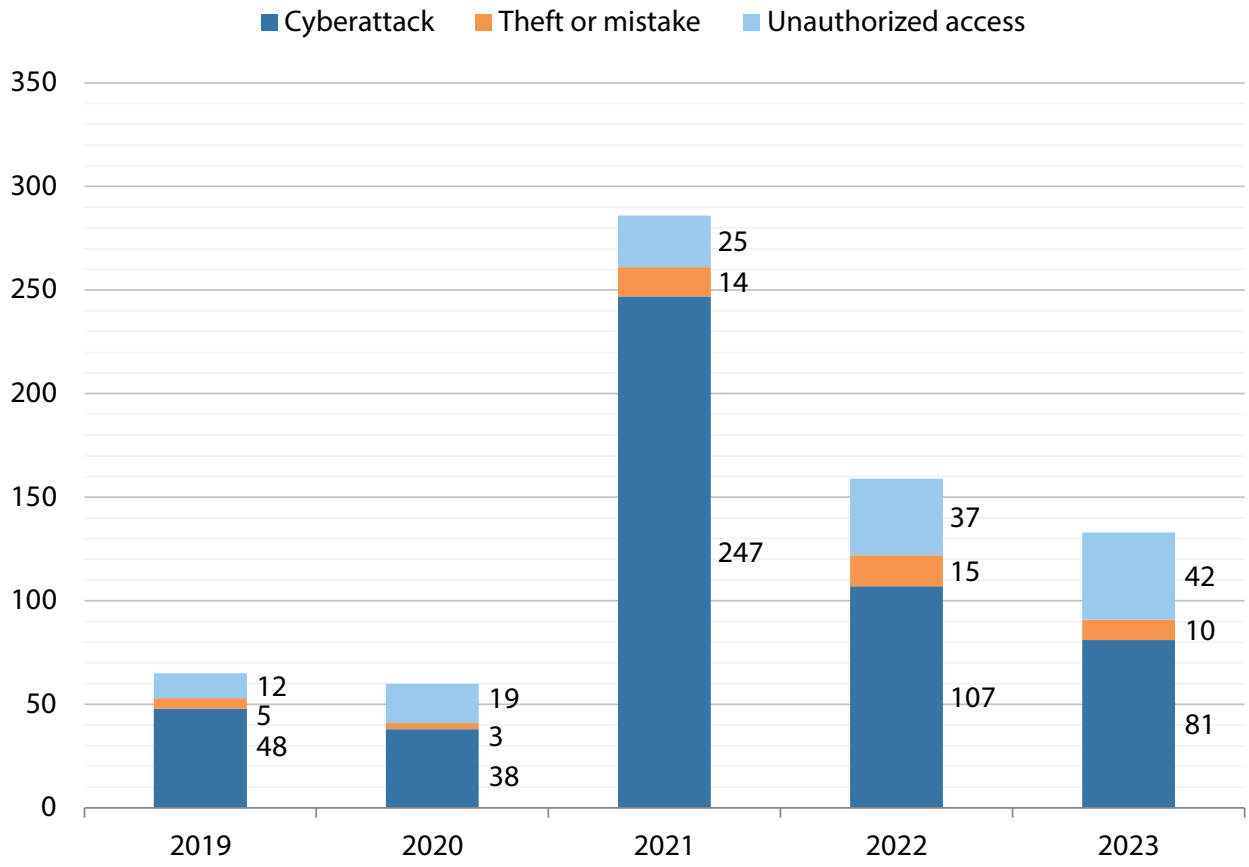
2. Expand language access requirements for data breach notifications;

3. Expand 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; and

4. Require more transparency from data brokers and data collectors so Washingtonians know more about businesses that store and sell personal data, how they operate, and the consumer information these entities control.

For detailed information on each of these recommendations, please see the "Recommendations" section on page 8.

## Total Number of Data Breaches by Cause

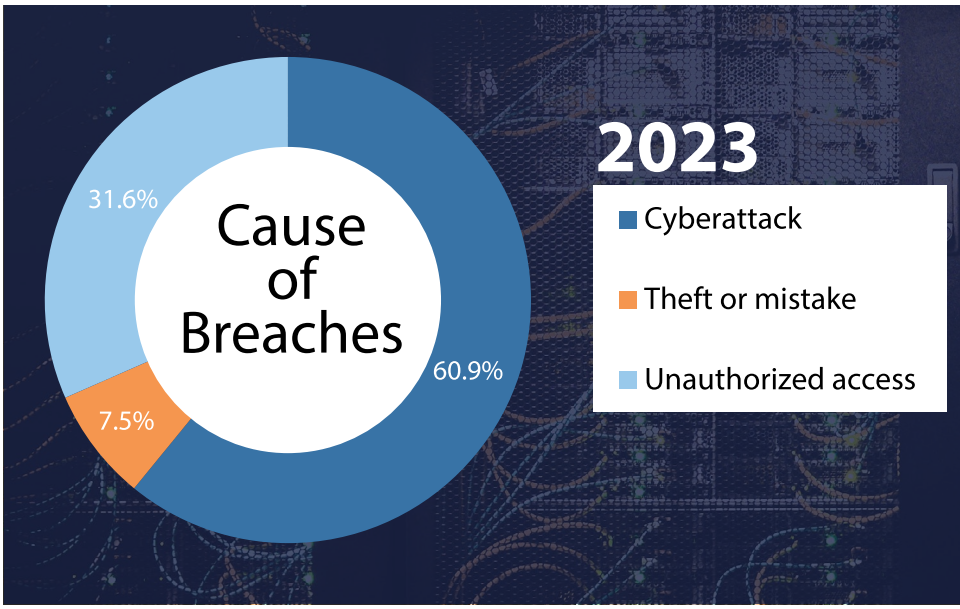



Data breaches fall into three broad categories:

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.

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.



# A Closer Look at Cyberattacks

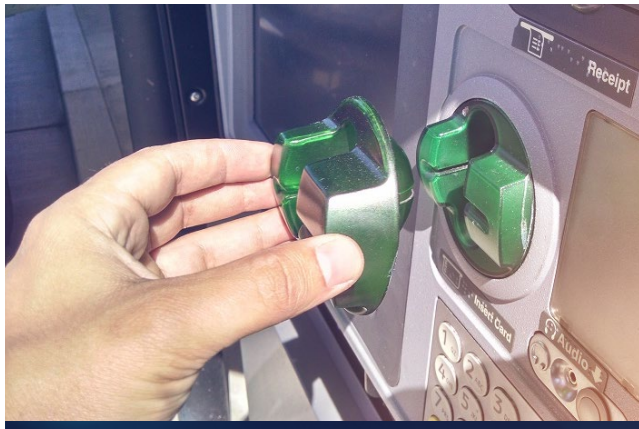
Cyberattacks can occur in a number of ways. Some of the most common methods include:

- Malware: The installation of malicious code onto a website, server, or network in order to disrupt the system or covertly obtain access to the data held within.

- Ransomware: A unique type of malware that holds data hostage while seeking a ransom payment from the breached entity. Typically, cybercriminals insert malicious code that encrypts data into an entity's network, thus locking the entity out of their own data.

- Phishing: The practice of sending a fraudulent communication, often via e-mail, that appears to be from a financial institution, government, employer, or other entity in order to fool the recipient into providing their information, or to download malware through an attachment or included link.

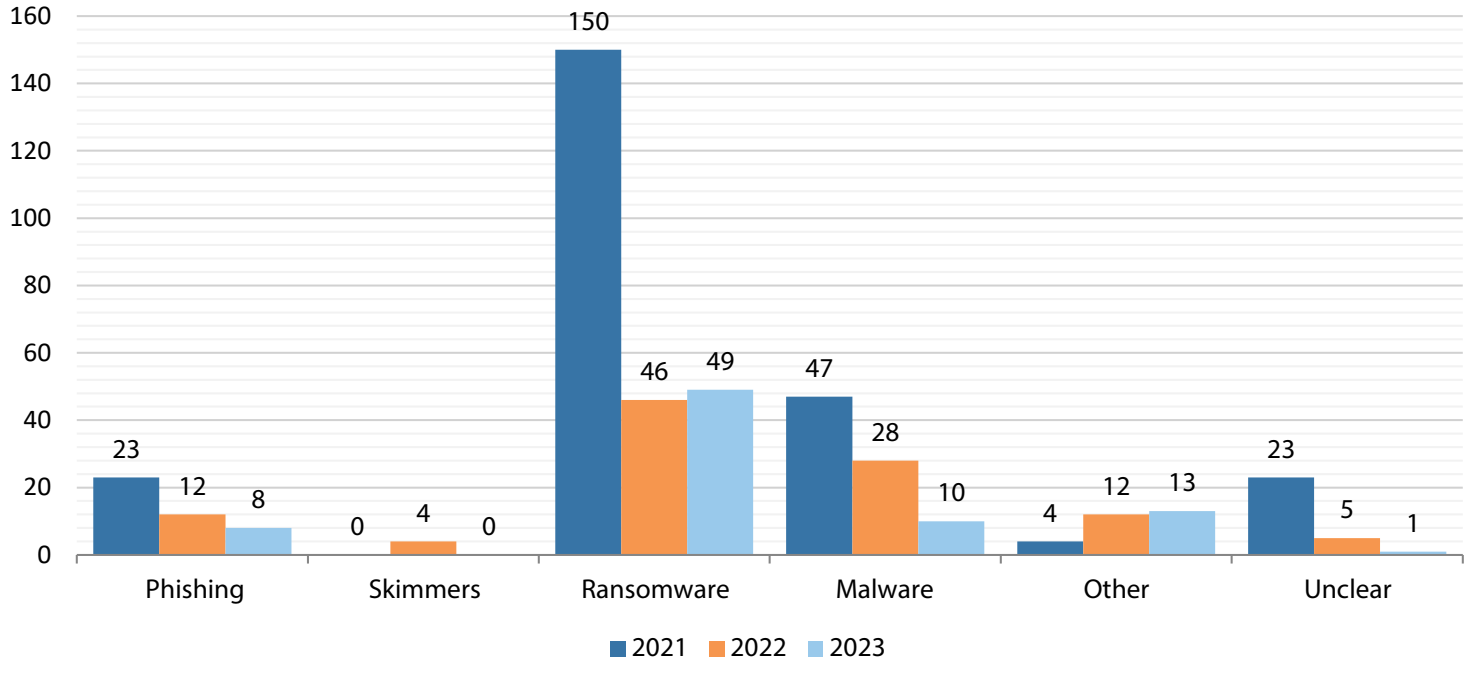
- Skimmers: A malicious card reader attached to payment terminals, such as those at an ATM or gas station, which collects data on cards inserted into the terminal. Often, cybercriminals will use the skimmer in conjunction with a device to record PIN information, such as a fake PIN pad or hidden camera.



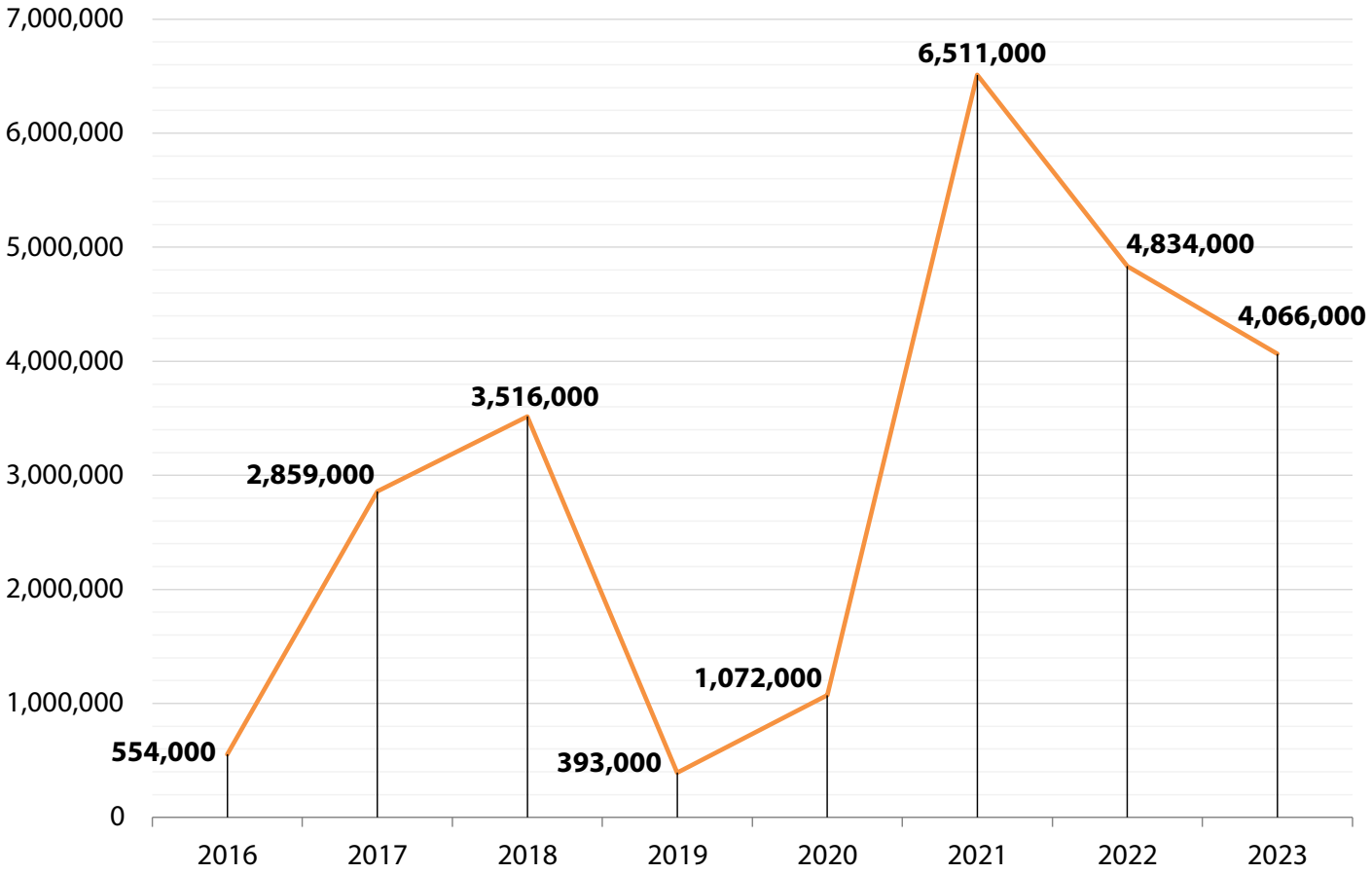

**A skimmer being installed on an ATM**
*Source: Washington State Department of Financial Institutions*

Our office was notified of 81 breaches caused by cyberattacks in 2023. Of those 81 breaches, one notice did not provide enough information to discern the specific method of cyberattack used. The most common cyberattack type was ransomware, which represented 61% (49 of 81) of cyberattacks. This is the third consecutive year in which ransomware attacks were the most common type of cyberattack.

## Malicious Cyberattacks by Type in Washington



## Annual Number of Washingtonians Affected by Data Breaches Since 2016




In 2023, 133 data breaches that affected more than 500 Washingtonians' personal information were reported to the AGO. This is down from 159 breaches in 2022. The total number of Washingtonians affected decreased as well – down 16% from last year, from 4,834,000 to approximately 4,066,000. Some statistics that stand out include:

- The overall number of reported breaches remains high at 133, more than double the average from 2016 through 2020 (61);
- The number of breaches impacting more than 50,000 Washingtonians is in double digits for the third straight year (10); and
- The overall number of Washingtonians affected decreased by only 16% from 2022, despite the fact that no mega breaches affecting more than one million Washingtonians were reported in 2023, while 2022's total includes a mega breach that affected more than 2 million residents (T-Mobile).

The 4,066,000 Washingtonians impacted in 2023 represent the third highest total affected by breaches in a single year since our office began tracking this information, demonstrating that data breach activity and severity remains a significant threat to consumers' data. Overall, the number of Washingtonians impacted by data breaches is rising consistently, with some variance depending on the number of breaches, in particularly the number of large entities suffering a data breach.

# Types of Personal Information Compromised

**Washington law requires notification to the AGO when a data breach includes personal information (PI). Washington defines PI as:[1]**

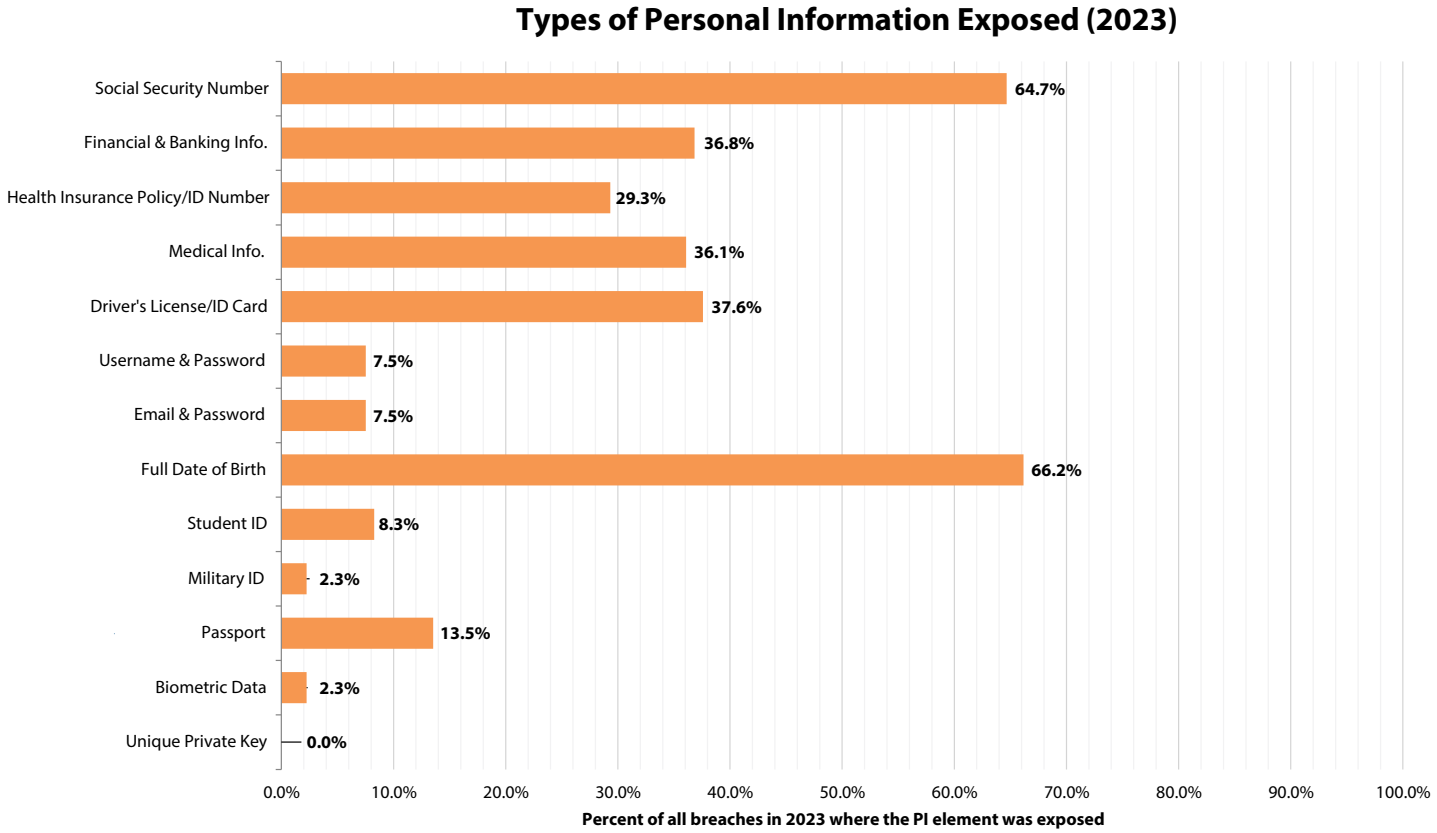
**An individual's first name or first initial and last name in combination with any of the following:**

- **Social Security number;**
- **Driver's license number or Washington identification card number;**
- **Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to their account, or any other numbers or information that can be used to access a person's financial account;**
- **Student, military, or passport identification numbers;**
- **Health insurance policy or identification numbers;**
- **Full date of birth;**
- **Private keys for electronic signature;**
- **Medical information, including medical history, mental or physical condition, diagnoses, or treatment; or**
- **Biometric data.**

**OR**

**An individual's username or email address in combination with a password or security questions and answers that would permit access to an online account.**

Additionally, any of the above elements, not in combination with first name or initial and last name, are considered PI if the affected data was not rendered unusable via encryption or redaction and would enable a person to commit identity theft against the consumer.


In 2023, 86 breaches, representing nearly two thirds (64.7%) of all breaches reported, resulted in the compromise of a Washingtonian's Social Security number (SSN). SSNs have been the second most commonly compromised piece of PI in seven of the last eight years. The only exception was 2022, when SSNs led this category.

Several of the new data points added to the data breach notification law in 2020, including birthdate, usernames and emails in combination with a password, and passport numbers, continue to appear in a significant number of breaches. Birthdate leads this category as the most commonly compromised piece of PI for the second time in three years.

# Recommendations

1. **Require businesses to recognize and honor opt-out preference signals.**

An opt-out preference signal, also sometimes referred to as a "Global Opt-Out," is a browser setting that, when enabled, automatically sends a signal to any website the consumer visits that they are requesting to opt-out of the business' sharing or sale of their personal information.

Opt-out preference signals are already in use around the world, such as the Global Privacy Control (GPC).[2] The GPC allows consumers to make a single opt-out request, by enabling the GPC in their browser, which applies to any and all websites they visit. However, not every jurisdiction requires businesses to honor these consumer requests. When businesses do honor these preference signals, they give consumers the power to efficiently assert their data sharing preferences. Without them, consumers are unfairly burdened with the task of manually opting-out of every single website they visit, and every service used by those websites, to request their information not be processed, shared, or sold.

Colorado's new data privacy law, the Colorado Privacy Act (CoPA), includes a requirement that businesses covered by the law must treat consumers' opt-out signals as a valid request to opt-out of the sharing and sale of their personal information.[3] This provision will go into effect on July 1, 2024. By January 1, 2024, the Colorado State Department of Law (Attorney General) will release an approved public list of global opt-out signals. Failure to honor these requests will be subject to fines under the Colorado Consumer Protection Act, which can range from $2,000 to $20,000 for each violation.

California's privacy law, the California Consumer Protection Act (CCPA), also requires businesses to honor consumers' opt-out preference signals. However, the California Privacy Rights Act, which went into effect on January 1, 2023, goes even further.[4] In addition to requiring businesses to honor a consumer's opt-out preference signal, businesses must give preference to opt-out signals in the event that a user has provided conflicting preferences (e.g. cookies preferences, or website settings). This means businesses are required to take the most conservative approach possible when determining if a consumer has given consent to share or sell their data. This contrasts with Colorado's law, which gives deference to other preferences over the opt-out signal. Additionally, businesses may also inform the consumer that they have received their global opt-out signal, addressing any ambiguity about whether the consumer's signal has been received.

If Washington's lawmakers require businesses to honor opt-out signals, Washingtonians will gain a powerful tool to control their data and reduce the risk that a breach will expose their personal information, thereby reducing the impact of future data breaches. Washington residents deserve the same protections and autonomy over how and whether their data is shared and sold, as the residents of these other states.

2. **Expand language access to data breach notifications.**

According to the Office of Financial Management (OFM), 20% of households in Washington State speak a language other than English.[5] English is spoken less than "very well" in 7.6% of Washington households. Despite this, there is no requirement for breached entities to provide notice in a language other than English.

Affected residents who do not receive information about risks to their data are less likely to be able to take the steps necessary to protect themselves and their information. It is imperative that all Washingtonians have an opportunity to receive notice in their native language. In order to address this inequity, the Legislature should consider adopting either of the following policy proposals:

a) Amend RCW 19.255 and RCW 42.65.590 to require breached entities to provide language accessibility options to impacted consumers, such as providing a phone number for an individual to call to speak with an interpreter, at no cost to the consumer; or

b) Require data breach notices be provided in any language that a breached entity advertises their products or services in.

3. **Expand the definition of "personal information" in RCW 19.255.005 to include:**

    a. Full name in combination with a redacted SSN that still exposes the last four digits of the number, bringing it into alignment with RCW 42.56.590; and

    b. Individual Tax Identification Numbers (ITINs).

The Legislature recently expanded the definition of "personal information" to cover the combination of name and the last four digits of Social Security numbers for breaches of a government agency, but did not make the same change to breaches of businesses.[6] The Legislature should bring the definitions into alignment, and provide consumers with more robust protections.

The Internal Revenue Service assigns ITINs to foreign-born individuals who are unable to acquire a Social Security number for the purposes of processing various tax related documents. In other words, they are a unique identifier equivalent in sensitivity to a Social Security number. At present, eleven states include ITINs in their definition of "personal information."[7]

In 2018, Washington State was home to just over 1.1 million foreign born individuals, representing approximately 15% of the state's population.[8] All Washingtonians deserve the same protection for their sensitive data, regardless of whether they have Social Security numbers or ITINs.

4. **Require transparency from data brokers and data collectors.**

Data brokers are businesses that specialize in collecting, aggregating, and selling consumer data. These firms often gather information from a range of sources, including public records, online activities, and purchase histories. This collected data is processed and repackaged into individual consumer profiles. These profiles can include information about an individual's demographic information, physical location, past purchases, websites visited, apps used, or even the content they consume online (e.g. YouTube channel subscriptions). These profiles are then sold to other businesses for a variety of purposes, including targeted advertising, credit scoring, and market research.
To better protect consumers, lawmakers should consider legislation to require data brokers and controllers to report annually to individual consumers, via physical or electronic mail, what information they presently hold, what information they have shared or sold and to whom, in language that is clear and accessible.

Additionally, lawmakers should require data brokers to:

a) Register and obtain a license with the state and subject itself to oversight, such as providing regulators with information about the sources of their data, the type of data they collect, how it is processed, who they sell it to, and for what purposes;[9]

b) Have strict data security measures (e.g. data security incident response team, ransomware prevention measures, etc.) in place before they can register with the state;

c) Publically disclose its policies for allowing consumers to opt-out of data processing; and

d) Pay a significant fine, and suspension of data broker license for violations of the above regulations.[10]

# Special Thanks

The completion of this report would not have been possible without the work and support of multiple AGO staff, namely:

- Cooper Smith, Policy Team
- Ellen Austin Hall, Policy Team
- Sahar Fathi, Policy Team
- Anthony Pickett, Administration
- Judy Gaul, Administration
- Mike Webb, Administration
- Donnelle Brooke, Consumer Protection Division
- Rabi Lahiri, Consumer Protection Division
- Joe Kanada, Consumer Protection Division
- Andrea Alegrett, Consumer Protection Division
- Brionna Aho, Public Affairs
- Ian Couch, Public Affairs
- Josh Manning, Public Affairs

# Resources for Individuals Affected by a Data Breach or Identity Theft

## First Steps

If you have just received notice that your data was involved in a data breach, consider taking these two important steps:

1 ***Place a fraud alert and security freeze on your credit reports.***

You can a place a fraud alert with one phone call. This can help prevent cyber criminals from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts, and all three credit reports will be sent to you free of charge. Once you receive the reports, review them carefully for accounts you didn't open, debts you can't explain or inaccurate information.

More information on how to place a fraud alert or credit freeze can be found here: https://www.atg.wa.gov/credit-freeze-fraud-alerts

2 ***Monitor your financial accounts, billing statement and credit reports for any suspicious activity.***

You may request a free annual credit report from each of the major nationwide credit bureaus at www.annualcreditreport.com or call 1-877-322-8228.

## Mitigating Identity Theft

Our office has information on steps you can take to mitigate your risk of identity theft. Many of these same principles also apply for mitigating your risk of having your data breached. You can find this info here: https://www.atg.wa.gov/protecting-personal-information

Additionally, if you have been notified that your data was exposed in a data breach, and you suspect you may have had your identity stolen as a result, consider consulting our office's guide on recovering from identity theft here: https://www.atg.wa.gov/recovering-identity-theft-or-fraud

Alternatively, you could also report your situation directly to the FTC online at identitytheft.gov. This website will not only record your report, but also has tools to help you develop a personal recovery plan and put it into action.

You might also consider reporting your situation with your local police department, as well as asking businesses to provide you with information about suspicious transactions made in your name. A template letter you can complete and send to businesses to request records can be downloaded here: https://www.atg.wa.gov/db-letter

## Resources for Businesses and Agencies

Any organization entrusted with individuals' information is potentially susceptible to a data breach. The AGO provides the following resources to help inform businesses on steps they can take to secure the data they hold and protect it from being breached.

Below are some basic steps that businesses can take to protect consumers' personal information:

- Understand your business' needs and how they relate to data security. This includes knowing what information you collect about consumers or clients, and knowing what information you retain and how it is retained.
- Consider identifying if the data you hold is subject to RCW 19.255's definition of personal information.
- Minimize the amount of information that you collect and retain. Delete any information that is no longer necessary. Consider reviewing RCW 19.215, "Disposal of Personal Information" for more details.
- Develop policies for the collection, encryption, and use of personal information.
- Create and implement an information security plan, including an action plan for steps to take in the event of a data breach. This could include developing a dedicated Incident Response Team, or implementing automated security technologies to detect attempted breaches.

*Resources for Businesses Responding to Data Breaches*

- FTC's "Protecting Personal Information: A Guide for Business"
    - This guide provides more in depth information on the basic steps outlined above for protecting consumers' data
- FTC's "Data Breach Response: A Guide for Business"
    - This guide provides critical information detailing what a business should do upon learning that their data security systems have been breached
- FTC's "Privacy and Security" webpage
    - This webpage provides valuable information about existing Federal data privacy laws, including additional resources for businesses
- Better Business Bureau's Cybersecurity HQ
    - This webpage contains business education resources for small and midsize businesses to help them manage cybersecurity risks and learn about best practices
- Internet Crime Complaint Center (IC3)
    - IC3 is the Nation's central hub for reporting cybercrime, and also provides resources such as industry alerts to help keep businesses aware of recent cybercrime trends.
- Cybersecurity & Infrastructure Security Agency's "I've Been Hit By Ransomware!" guide
    - This guide provides step-by-step instructions for businesses to take after being hit with a ransomware attack.
- Cyber Readiness Institute's Ransomware Playbook
    - This guide provides businesses with information on how to prepare for, respond to, and recover from ransomware attacks.

# Data Analysis Methodology & Limitations

In assessing data breach notification data, it is important to acknowledge the nature and limitations of collecting and analyzing this information.

Data breaches are a moving target. Notices to the AGO are often sent with incomplete information, and can be updated with new facts months after an initial notice. While some of this can be attributed to human error in how the information is reported, it is also a product of how complicated and time-intensive resolving and understanding data breaches can be. This is particularly true if the breached organization does not have a dedicated cybersecurity team on staff and, consequently, must contract out its analysis and containment measures. As such, it is important to keep in mind that the data provided in this report is a point-in-time snapshot of what we know. Put simply, the statistics in this report are estimates. The data in this year's report is a snapshot of what we know as of September 1, 2023.

In 2021, our office built a new data collection system for data breach notices, as well as a standardized online web form for breached organizations to provide notice to the AGO. Since implementation, this form has led to improved accuracy and completeness of notices regarding data breaches affecting Washingtonians, as well as a more efficient notification process for everyone involved. We hope more organizations will utilize this process going forward. This web form is available at: https://fortress.wa.gov/atg/formhandler/ago/databreachnotificationform.aspx.

Additionally, this live updating database provides our office a powerful tool for auditing and updating past years' data. As such, the AGO has revised several statistics reported in past years with more complete and accurate information. Of particular note, the total number of Washingtonians in 2022 increased from the 4.5 million figure we reported last October, to an updated total of 4.8 million.

Lastly, it is important that we clarify what this report means when we refer to the "Number of Washingtonians Affected." This statistic comes from the notices breached organizations provide to our office, which must include the total number of Washington residents the organization notified of its data breach. This figure is a sum of all the data breach notices sent to Washingtonians, and may not necessarily reflect the exact number of individual Washingtonians impacted by data breaches in a given year. This is because multiple breaches can affect a single Washingtonian. In other words, it is possible for a single Washington resident to receive multiple data breach notices, and thus appear multiple times within our dataset. However, because this is the single best indicator we have of estimating the numerical impact to residents of our state, we refer to it as the "Number of Washingtonians Affected."

# Notes & Citations

1 RCW 19.255.010, effective since March 2020. https://app.leg.wa.gov/RCW/default.aspx?cite=19.255.010.

2 Global Privacy Control. Accessed October 2022, from https://globalprivacycontrol.org/.

3 Colorado Revised Statutes, Title 6, Article 1, Part 13, 6-1-1306 (1)(a)(IV) https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.

4 California Code of Regulations, Title 11, Division 6, Chapter 1, Article 3, § 7025. https://govt.westlaw.com/calregs/Document/IFA415050D45011EDA6283814282AA05E?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default).

5 Office of Financial Management. (2022, August 19). "Language spoken at home." Accessed August 2022, from https://ofm.wa.gov/washington-data-research/statewide-data/washington-trends/social-economic-conditions/language-spoken-home.

6 There is no other state that includes redacted Social Security Numbers (SSNs) in their definition of Personal Information. The only other state that does something different than name in combination with SSN is Indiana, where breaching an SSN by itself triggers their law (no name needed).

7 Alabama, Arizona, California, Connecticut, Delaware, Maryland, Montana, North Carolina, Vermont, Virginia, Wyoming.

8 U.S. Census Bureau. (2020). "2020 American Community Survey 5-Year Estimates Data Profiles." Accessed August 2022, from https://data.census.gov/cedsci/table?q=DP02#.

Two states explicitly name Tribal IDs as protected information requiring a data breach notice: Rhode Island & Wyoming.

9 In California, data broker registration goes through the Attorney General's Office: https://oag.ca.gov/data-broker/register. In Vermont, registration goes through the Secretary of State: https://sos.vermont.gov/corporations/other-services/data-brokers/.

10 The General Data Protection Regulation (GDPR) allows each member state's data regulator to fine violators up to 4% of global annual revenues of the preceding year or 20 million euros, whichever is higher. For any potential Washington data broker law, defining a fine as a percentage is recommended so that it scales with inflation over time.