WASHINGTON STATE ATTORNEY GENERAL'S OFFICE

2022

DATA BREACH REPORT

SPECIAL EDITION:
DATA PRIVACY

TABLE OF CONTENTS

Letter from the Attorney General 1

The Intersection of Data Breaches & Data Privacy 2

Executive Summary 3

Causes of Data Breaches 5

A Closer Look at Cyberattacks 6

Number of Washingtonians Affected 7

Types of Personal Information Compromised 10

Industries Reporting Breaches 12

Time to Resolve Data Breaches 14

Washington's Data Breach Notification Law - The Strongest in the Country 17

Recommendations 21

Appendix 24

- Resources for Individuals & Businesses 24
- Washington's Data Breach & Data Security Laws 25
- Data Analysis & Methodology 26
- Special Thanks 27
- Notes and Citations 28

LETTER FROM THE ATTORNEY GENERAL

October 2022

Dear Washingtonians,

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.

In 2022, Washingtonians experienced the second most data breaches (150) and the second highest number of Washingtonians impacted by data breaches (4.5 million) in a single year.

These numbers are staggering. The implications for Washingtonians' privacy rights is significant. As such, in this report, the seventh annual Data Breach Report published by my office, we are doing something different.

Previous reports included recommendations for strengthening Washington's data breach laws. I proposed several of these recommendations as Attorney General Request legislation, and the Legislature adopted them. Thanks to these reforms, Washingtonians now have the strongest data breach notification protections in the country.

For years, my office has successfully blocked weak, ineffective data privacy legislation from passing the Washington Legislature. In this **special Data Privacy edition** of the Data Breach Report, I am taking the unique step of proposing legislative reforms to protect Washingtonians' data privacy.

This report includes recommendations that would protect Washingtonians' most sensitive data by:

- Protecting Washington consumers' health data privacy, an issue that has taken on increased urgency since the *Dobbs v. Jackson Women's Health Organization* decision; and
- Allowing consumers to use a single portal to opt-out of having their data shared or sold, also known as an "opt-out preference signal."

Current laws, such as the Health Insurance Portability and Accountability Act, do not provide a sufficient level of protection. That's why I am partnering with Representative Vandana Slatter (D-Bellevue) to propose new legislation to protect Washingtonians' health data privacy.

My office 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 more than $16 million**.

We will continue to enforce the law, and to work to ensure Washingtonians have the information needed to **protect your business and your data.**

Sincerely,

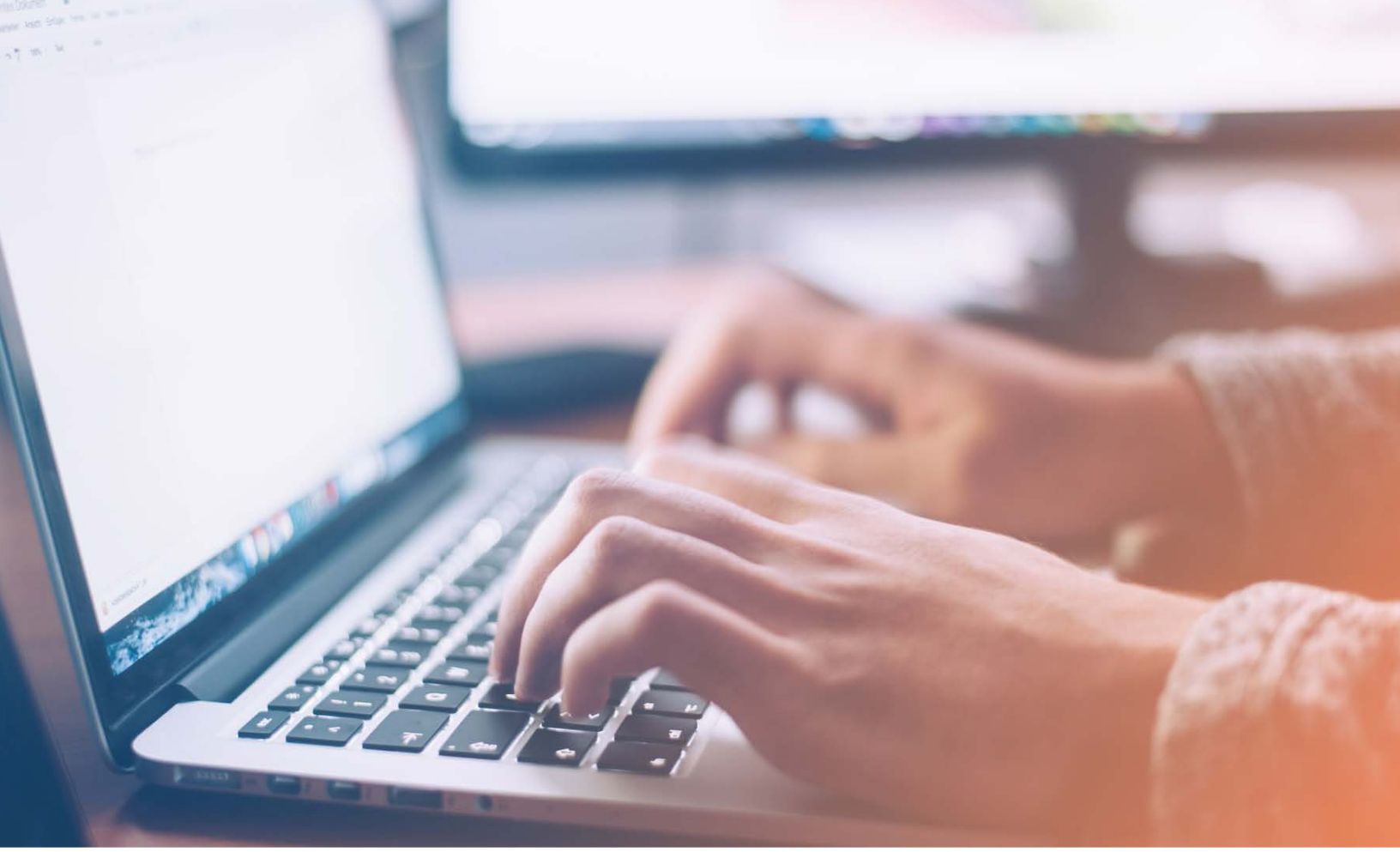
Bob Ferguson
Washington State Attorney General

The Intersection of Data Breaches & Data Privacy

The impact of data privacy practices and policies on the data breaches we cover is too large to ignore because data privacy and data breaches are two sides of the same coin. The data privacy field is about the laws, consumer rights, and industry practices that govern when, how, and who can collect, share, sell and delete the information that we interact with or provide, often unknowingly, in our day-to-day lives.

Data breaches generally occur when illegal actions of cybercriminals or the negligence of entities controlling personal information results in the violation of individuals' data privacy. However, due to the sheer amount of personal data collected, shared, and sold by businesses and other entities, cybercriminals are not necessary for data privacy violations to occur. Policymakers must urgently recognize this and act to establish meaningful protections for consumer data. Corporate practices of collecting, sharing and selling sensitive personal data can and do result in privacy violations. These practices may not involve illegal activity, although the potential harm to the consumer can be significant.

Every year our office provides several recommendations to better protect consumers from the harms caused by data breaches, and to strengthen data breach notification requirements. In this report, we also include legislative recommendations to provide Washingtonians more control over their data, and prohibit the sharing and selling of our most sensitive health data.



Executive Summary

- **2022 represents the second highest number of data breach notices sent to Washingtonians (4.5 million) since 2016.**
    - 2021 holds the record for highest number of notices at 6.5 million.

- **The AGO received 150 data breach notifications in 2022 – also the second highest recorded amount since 2016.**
    - This is half the size of last year's staggering record of 285 (2021), but is significantly more than double the 2016-2020 average of 61 notices per year.

- **Cyberattacks and ransomware attacks continue to be prolific in 2022.**
    - Cyberattacks caused 68% of all reported data breaches.
    - 43 data breach notices cited ransomware. This is down from the astounding 150 ransomware notices reported in 2021, but is still more than quadruple the total number reported between 2016 and 2020 (10).
    - Ransomware attacks accounted for 42% of all cyberattacks (43 of 102) and nearly a third of all breaches (43 of 150).

- **2022 saw another mega breach, following the cyberattack on Accellion last year.**
    - The T-Mobile USA mega breach, the second largest mega breach to affect Washingtonians since Equifax in 2018 (3.2 million), resulted in the exposure of just over two million Washingtonians' unencrypted personal information. The impacted files contained personal data, including residents' names, Social Security numbers, dates of birth, and government ID numbers.
    - The T-Mobile mega breach is the fourth since 2016, and the second time Washingtonians experienced mega breaches in consecutive years (2017-18 & 2021-22).

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 was 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 that notices to consumers 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, 2021 and July 23, 2022 that affected more than 500 Washingtonians' personal information. Additional information on our data gathering and analysis process is available in the "Data Analysis Methodology" section in the Appendix on page 26.

Recommendations

In order for policymakers to strengthen privacy and data breach protections for Washington residents, the Attorney General's Office recommends that they:

1. Pass legislation to protect consumers' private health data.

2. Pass legislation providing Washingtonians freedom to control their data by requiring organizations to recognize and honor opt-out preference signals.

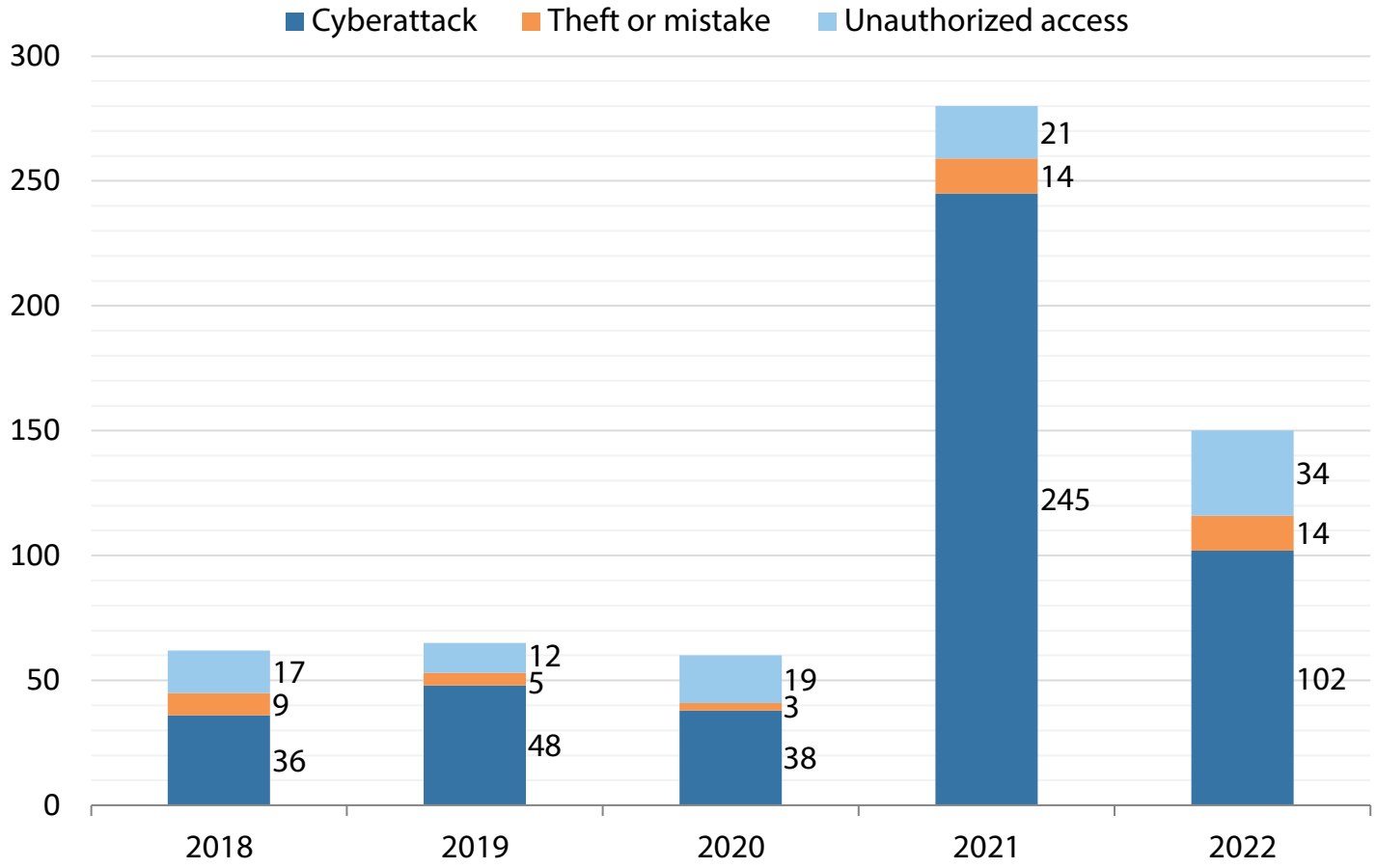
3. Expand language access to data breach notifications.

4. 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 and (b) Individual Tax Identification numbers (ITINs).

5. Require more transparency from data brokers and data collectors so Washingtonians know more about the consumer information these entities control.

For detailed information on each of these recommendations, please see the "Recommendations" section on page 21.

Total Number of Data Breaches by Cause

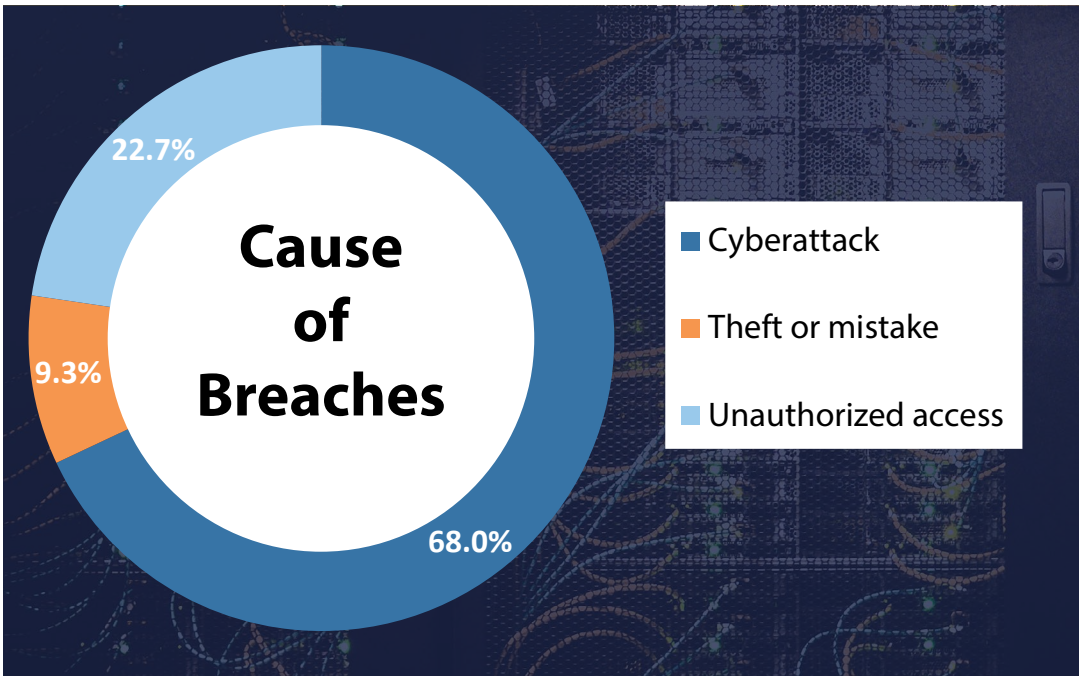


Data breaches fall into three broad categories:

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, ransomeware, 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.

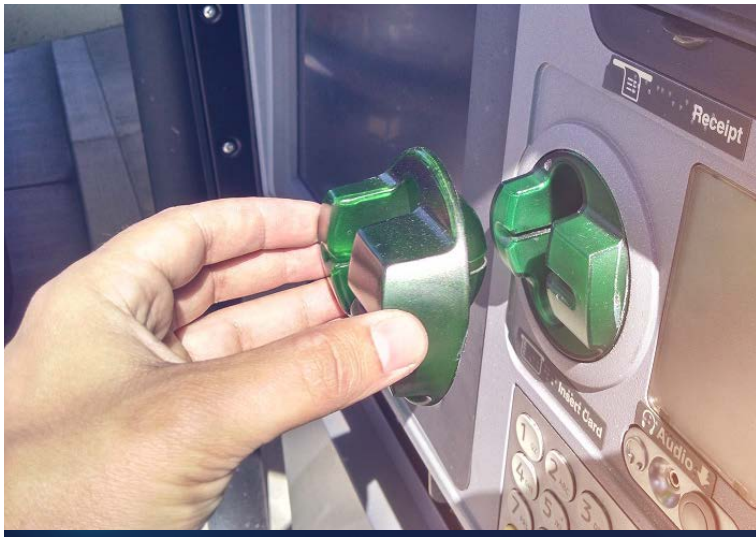
3. Unauthorized access: An unauthorized person purposefully accesses secure data through means such as an unsecured network or sifting through sensitive documents left out on a desk.



A Closer Look at Cyberattacks

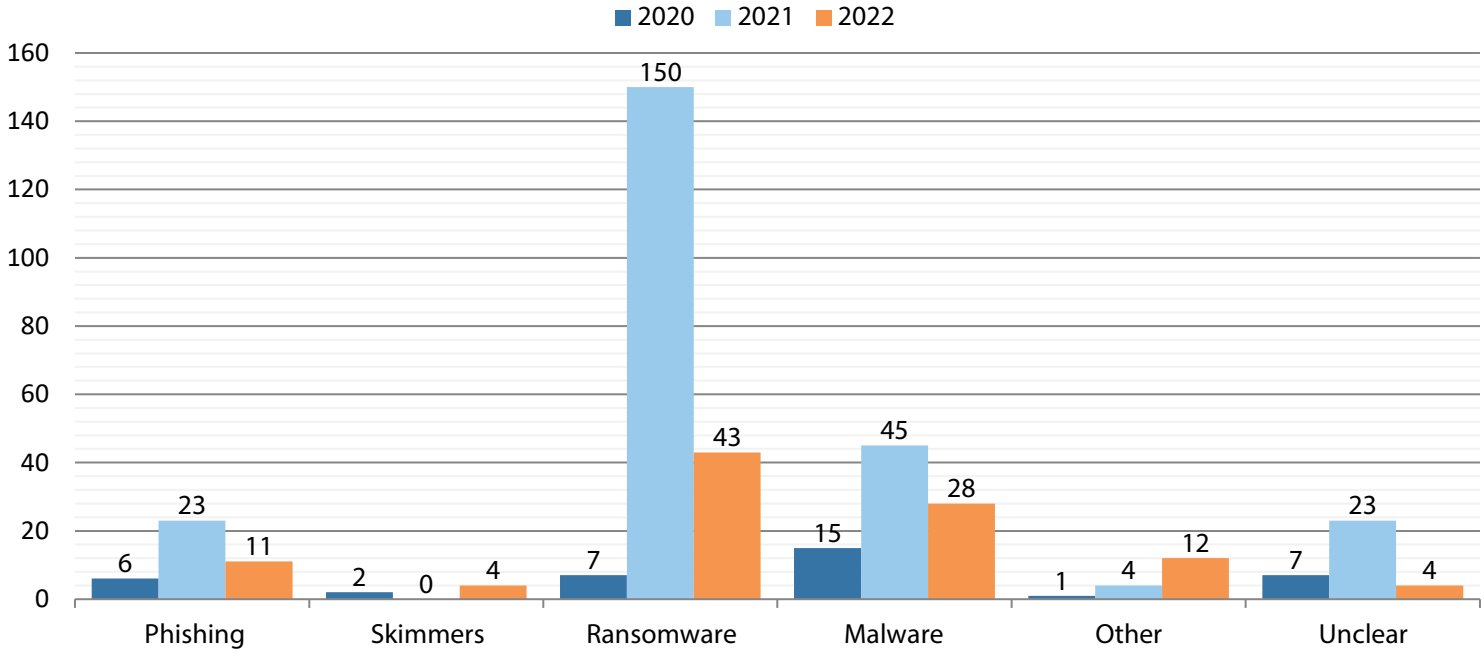
Cyberattacks can occur in a number of ways. Some of the most common methods include:

- 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 in hopes of receiving a ransom payment from the breached entity. Typically, cybercriminals will insert malicious code into a network that encrypts the data, and thus renders it inaccessible to the breached organization.
- Phishing: The practice of sending a fraudulent communication, often via e-mail, 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.



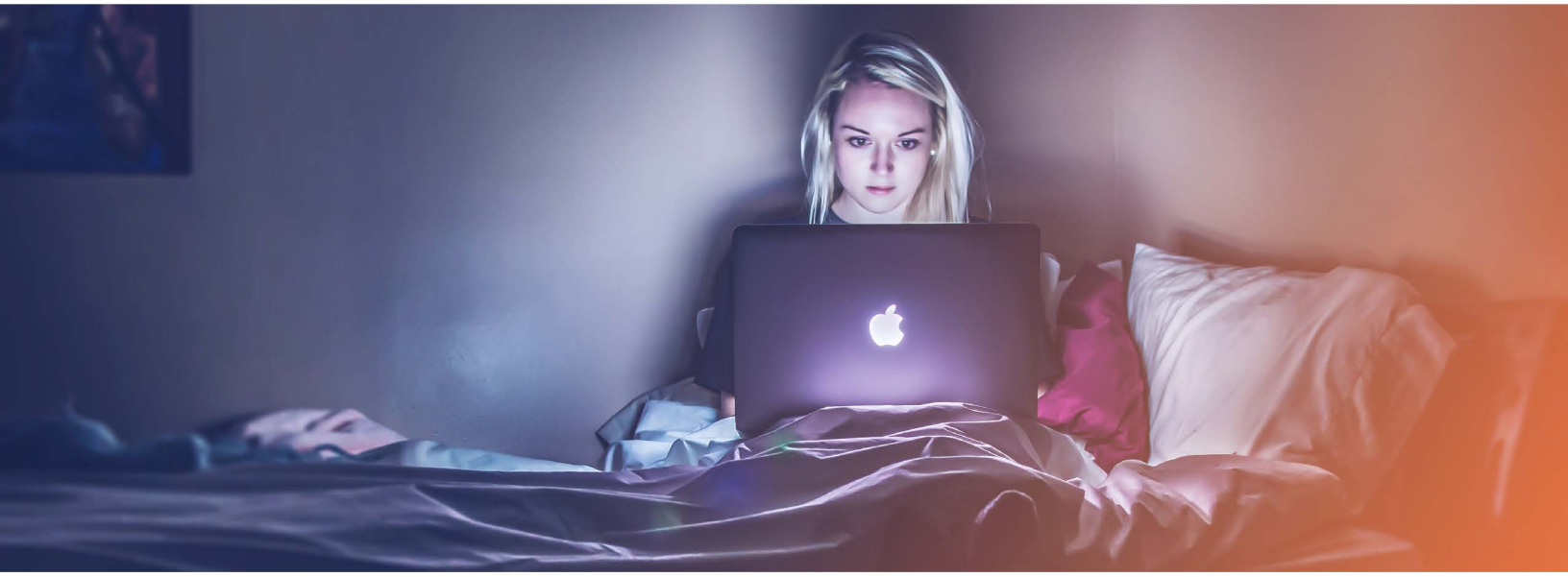
A skimmer being installed on an ATM
Source: Washington State Department of Financial Institutions

Malicious Cyberattacks by Type in Washington



Our office was notified of 102 breaches caused by cyberattacks in 2022. Of those 102 breaches, four of the notices did not provide enough information to discern the specific method of cyberattack used. The most common cyberattack type in 2022 was ransomware, which represented 42% (43 of 102) of cyberattacks. This is the second year in a row where ransomware attacks were the most common type of cyberattack, following last year's staggering 150 ransomware attacks.

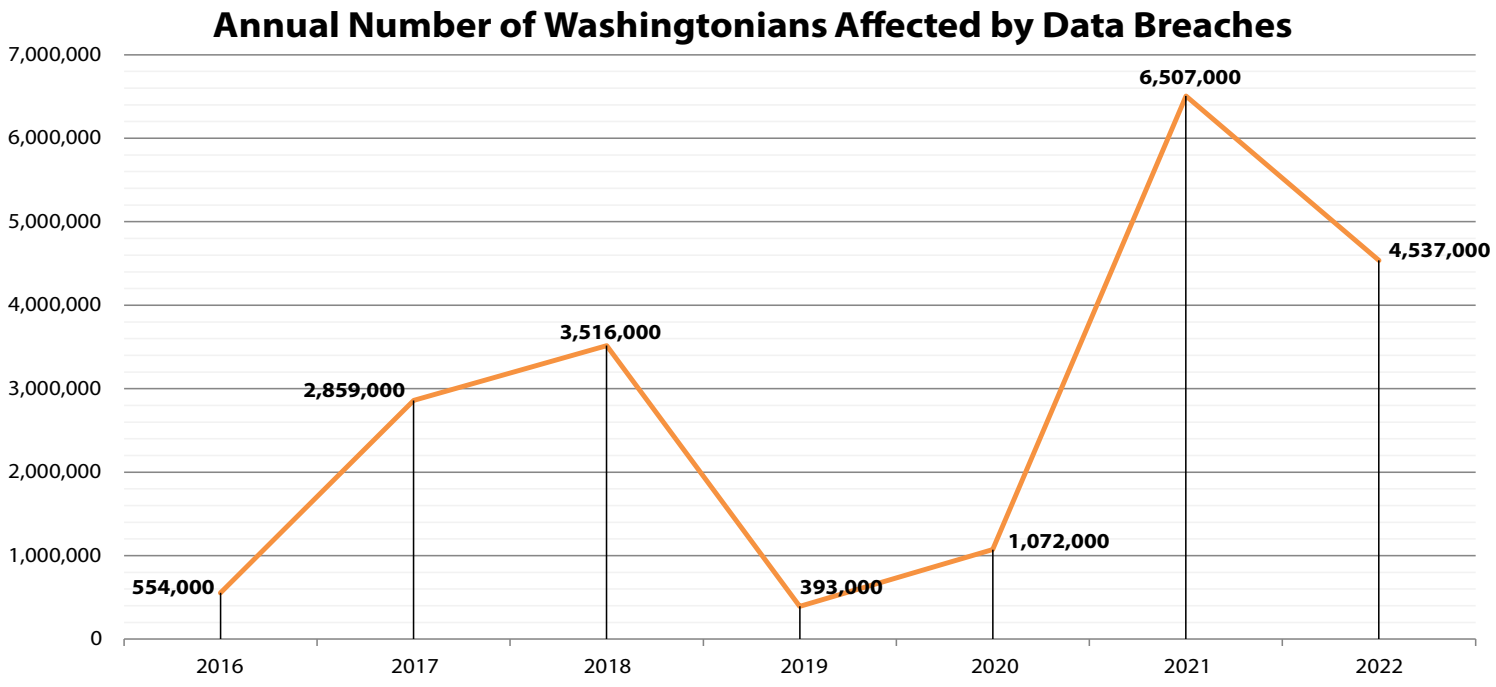
Number of Washingtonians Affected

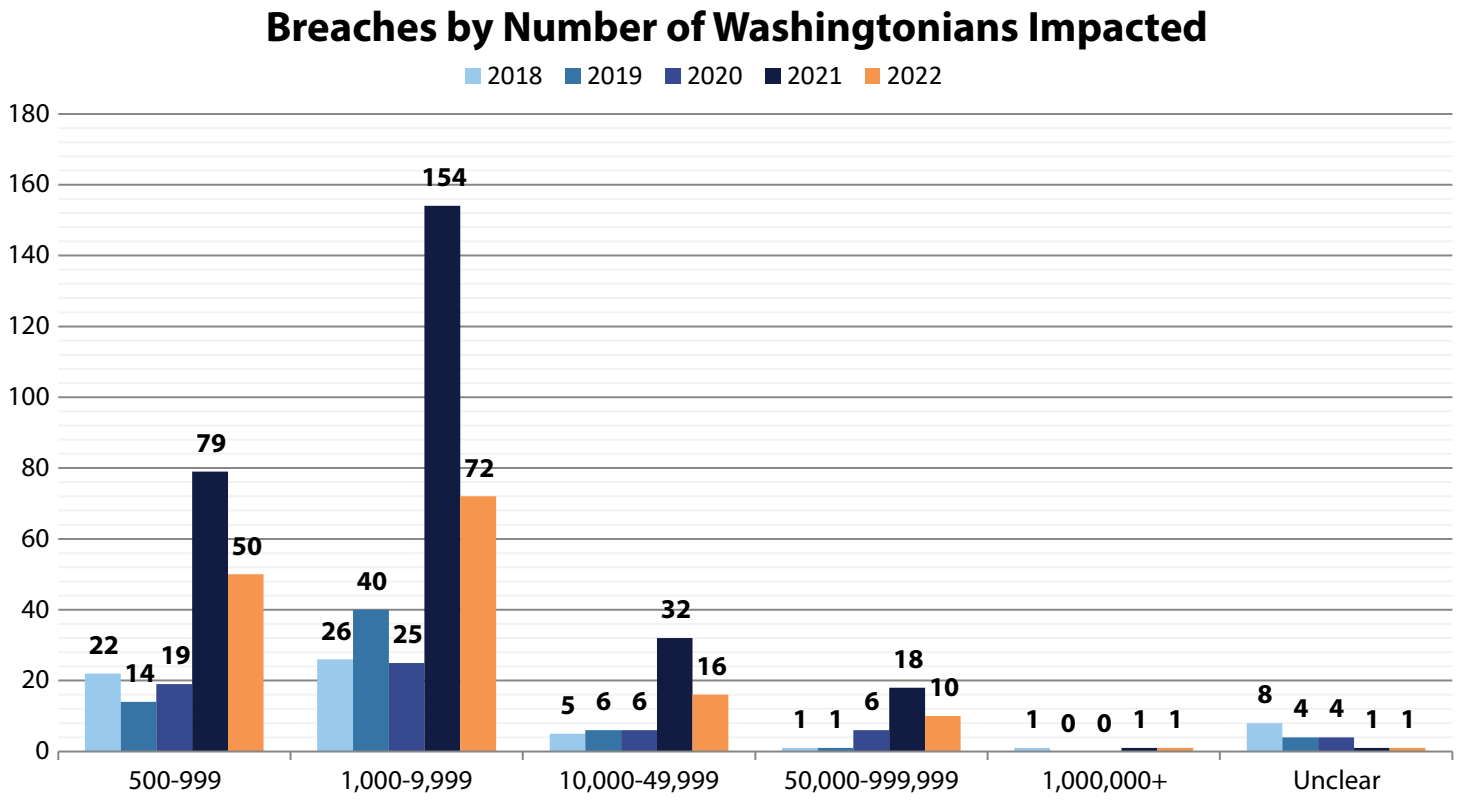


In 2022, 150 data breaches that affected more than 500 Washingtonians' personal information were reported to the AGO. This is down from 285 breaches in 2021. The total number of Washingtonians affected decreased as well – down 30% from last year, from 6,507,000 to approximately 4,537,000. Despite the reduction, this represents the second highest number of Washingtonians affected by breaches in a single year since our office began tracking this information.

While the torrent of breaches in 2021 may make 2022 look tame in comparison, the numbers still show that data breach activity and severity remains at historic highs:

- The overall number of reported breaches remains quite high at 150, which is 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 second straight year (10); and
- For the second year in a row, Washingtonians were impacted by a mega breach (T-Mobile) affecting more than one million residents. This is the second largest data breach (two million residents) to hit our state since this report began in 2016. Only the 2018 breach of Equifax was larger (3.24 million residents).

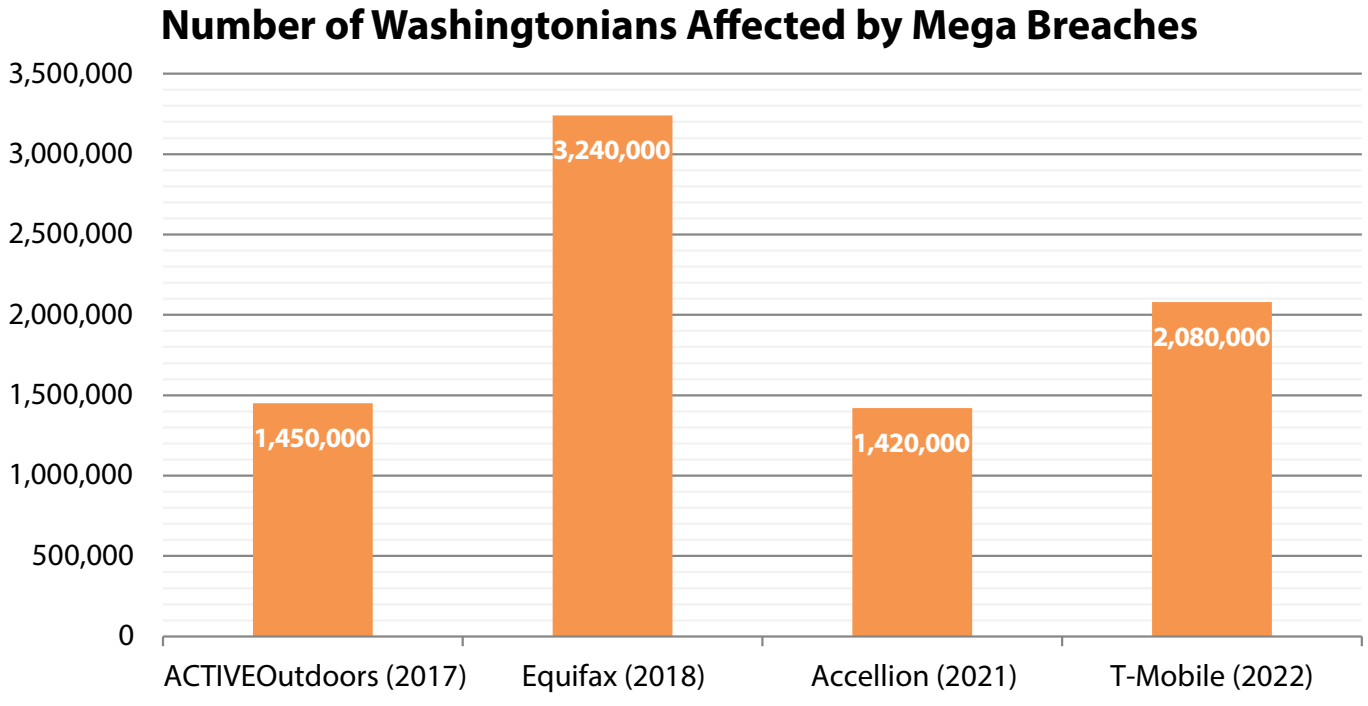




In 2022, the majority of data breaches compromised the personal information of between 1,000 and 9,999 Washington residents. This is the fifth straight year that the majority of breaches affected at least 1,000 Washingtonians.

What are "Mega Breaches"?

For the purposes of this report, a mega breach is any data breach that affects the personal information of one million or more Washington residents. When they occur, these breaches can impact more people in a single breach than the combined total from all other breaches in that year.



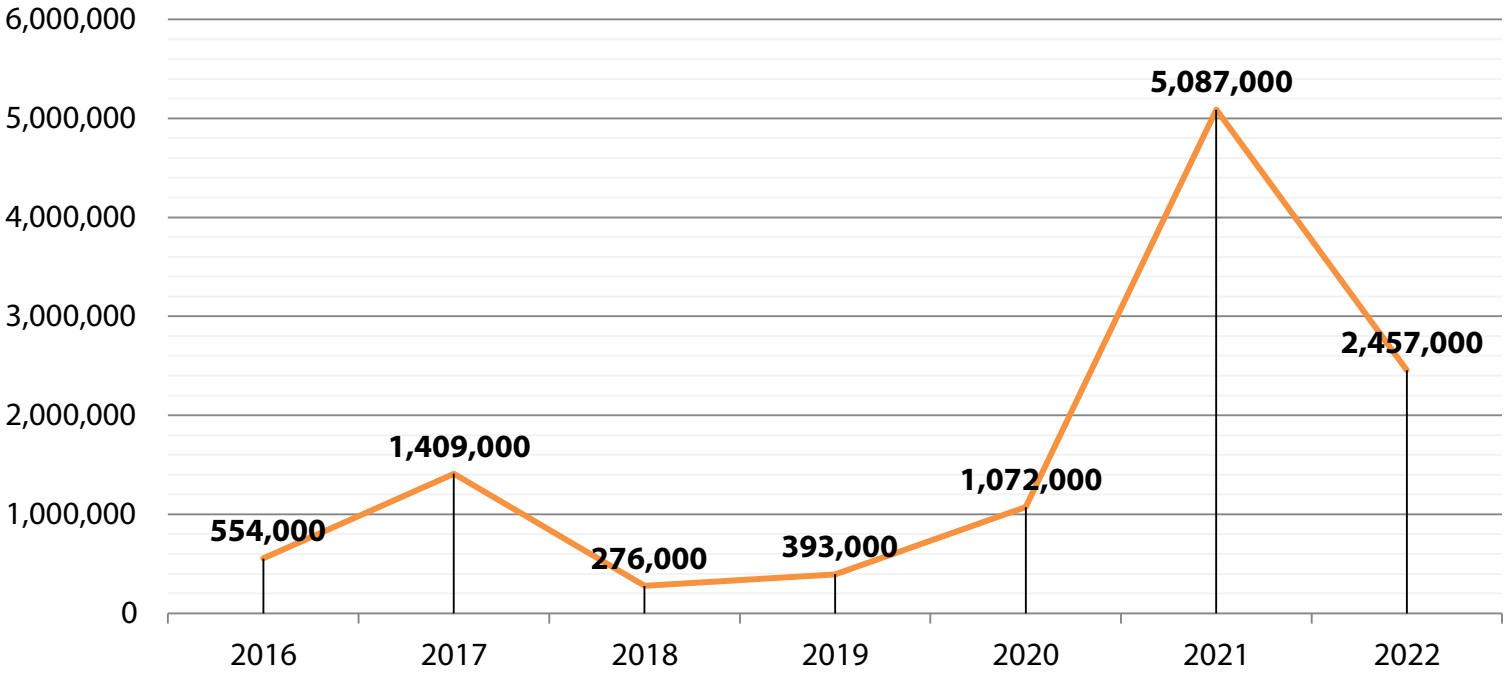
Since our office began issuing this report in 2016, four organizations reported mega breaches to the AGO– the ACTIVEOutdoors breach in 2017, the Equifax breach in 2018, the Accellion breach in 2021, and this year's breach of T-Mobile.

These breaches are significant not only because of the large number of consumers they impact, but also for the massive costs associated with resolving them. According to the Ponemon Institute's 2022 "Cost of a Data Breach Report," breaches compromising one to 10 million records cost breached entities an average of $49 million per breach, while breaches affecting more than 50 million records cost an average of $387 million per breach.[1] While the numbers reported in the chart are the number of Washingtonians affected, the total number of people impacted is much higher. The T-Mobile breach affected approximately 50 million consumers, and the Equifax breach affected 147 million.

The 2022 mega breach of T-Mobile significantly influenced this year's data, making up nearly half (46%) of all Washingtonians impacted by data breaches this year. Of great concern is that the stolen files were unencrypted, and contained various pieces of particularly sensitive data, including resident's names, Social Security numbers, dates of birth, and government ID numbers.

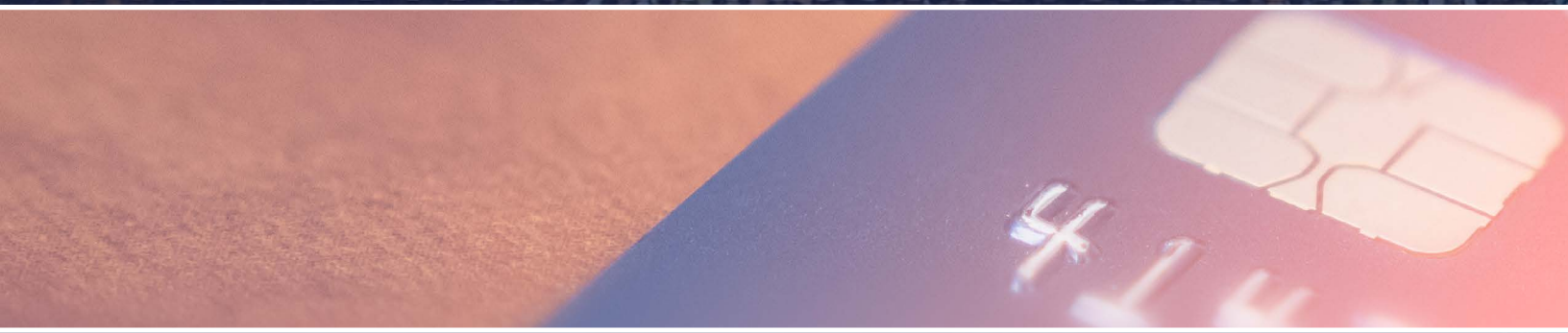
Due to their massive size, mega breaches like T-Mobile's can obscure trend data for the more common small to midsize breaches.

Annual Number of Washingtonians Affected by Data Breaches Not Including Mega Breaches



The chart above shows the number of Washingtonians affected by data breaches since 2016 with data from mega breaches removed. From this chart, we can see that without mega breaches, the total number of Washingtonians impacted increased by about one-half in 2019, and more than doubled in 2020. In 2021, the total number of Washingtonians spiked by an additional 374%, driven by a ransomware attack on the cloud-computing provider Blackbaud, which affected over 100 education and non-profit organizations. In 2022, this total dropped 52%, yet remains the second highest on record, demonstrating the continued threat data breaches pose to consumers and their privacy.

Types of Personal Information Compromised



Washington law requires notification to the AGO when a data breach includes personal information (PI). Washington defines PI as:[2]

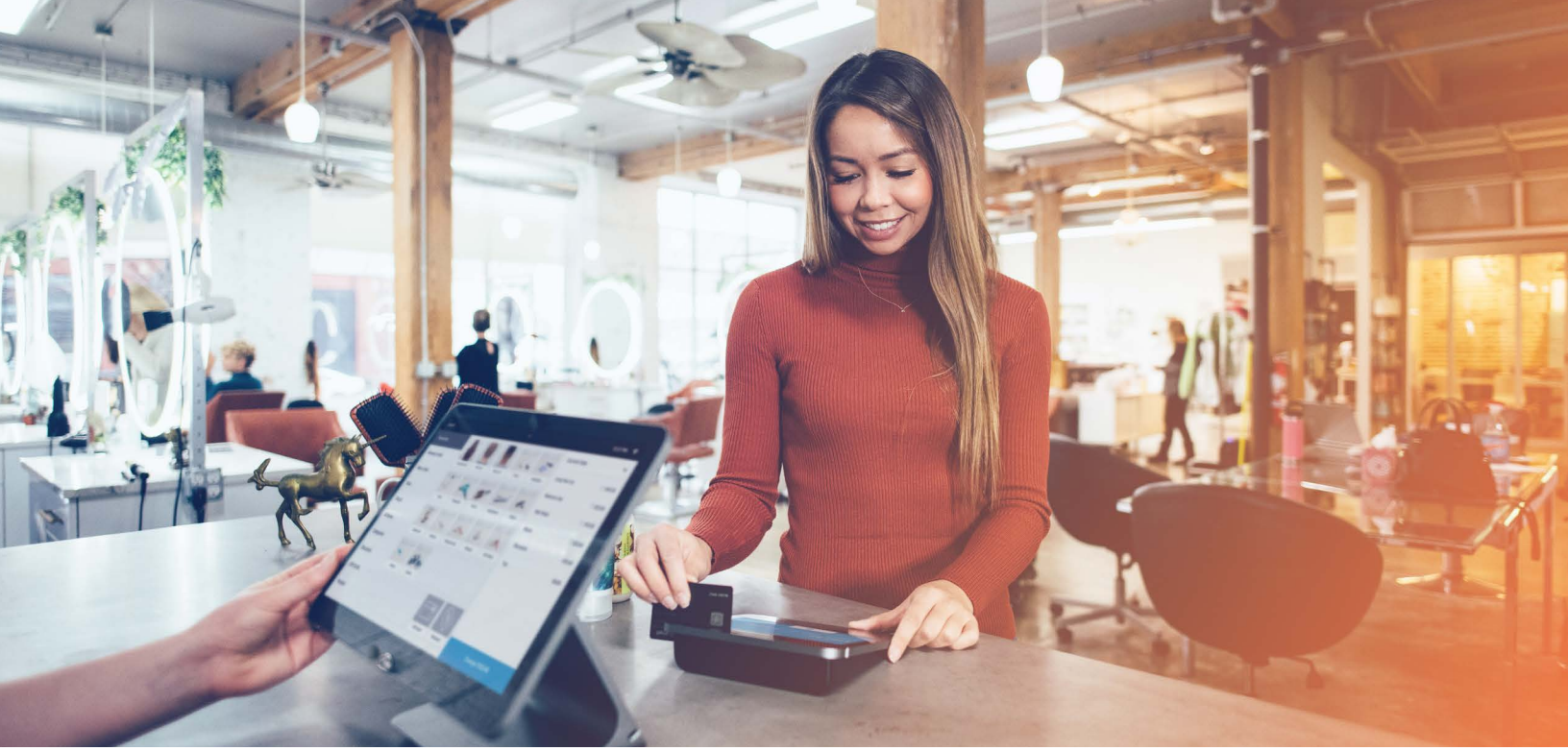
An individual's first name or first initial and last name in combination with any of the following:

- **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.**

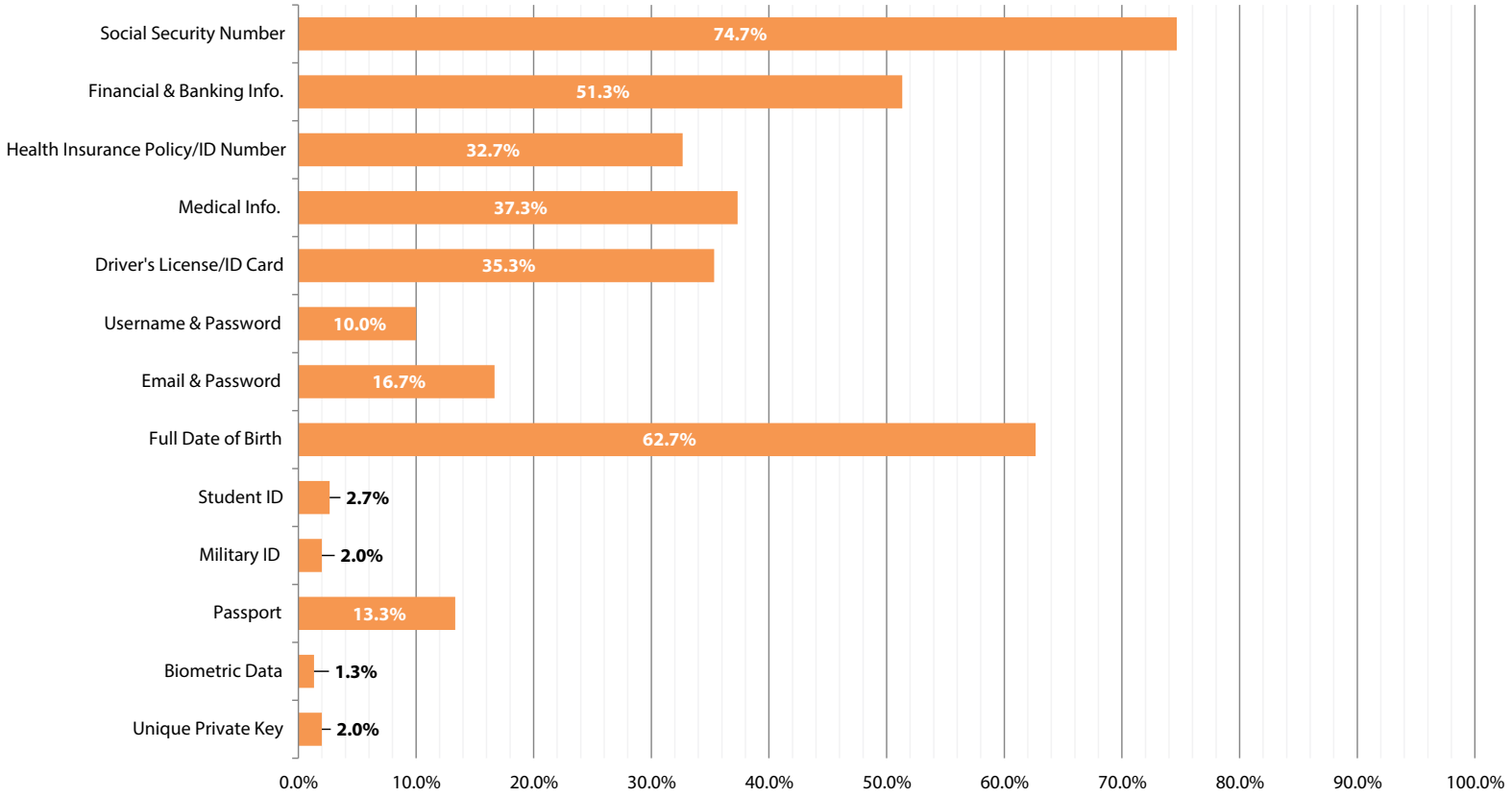
OR

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.



PI Exposure Percentages (2022)

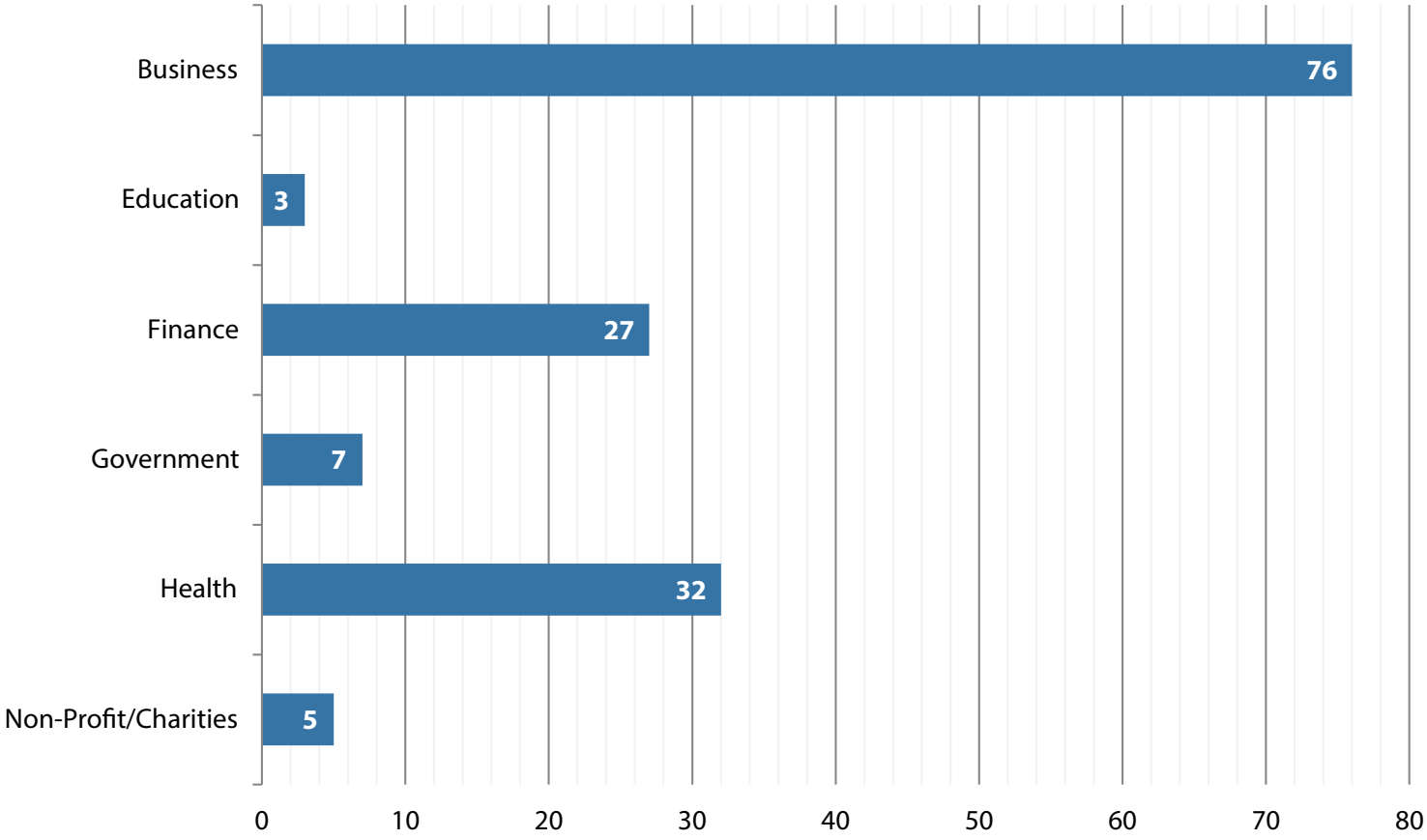


In 2022, 112 breaches, representing nearly three quarters (74.7%) of all breaches reported, resulted in the compromise of a Washingtonian's Social Security number. Social Security numbers were the second most commonly compromised piece of PI in each of the previous six years. This is the first time they lead this category.

Several of the new data points recently added to the data breach notification law as a result of the Attorney General's 2020 legislative update continue to appear in a significant number of breaches, including birthdate, username in combination with a password, and passport numbers. Birthdate stands out as the second most commonly compromised piece of PI.

Industries Reporting Breaches

Number of Breaches in 2022 by Industry



The AGO tracks breaches by industry. Consistent with earlier reports, our office uses the following industry categories:

Business

Education

Financial Services

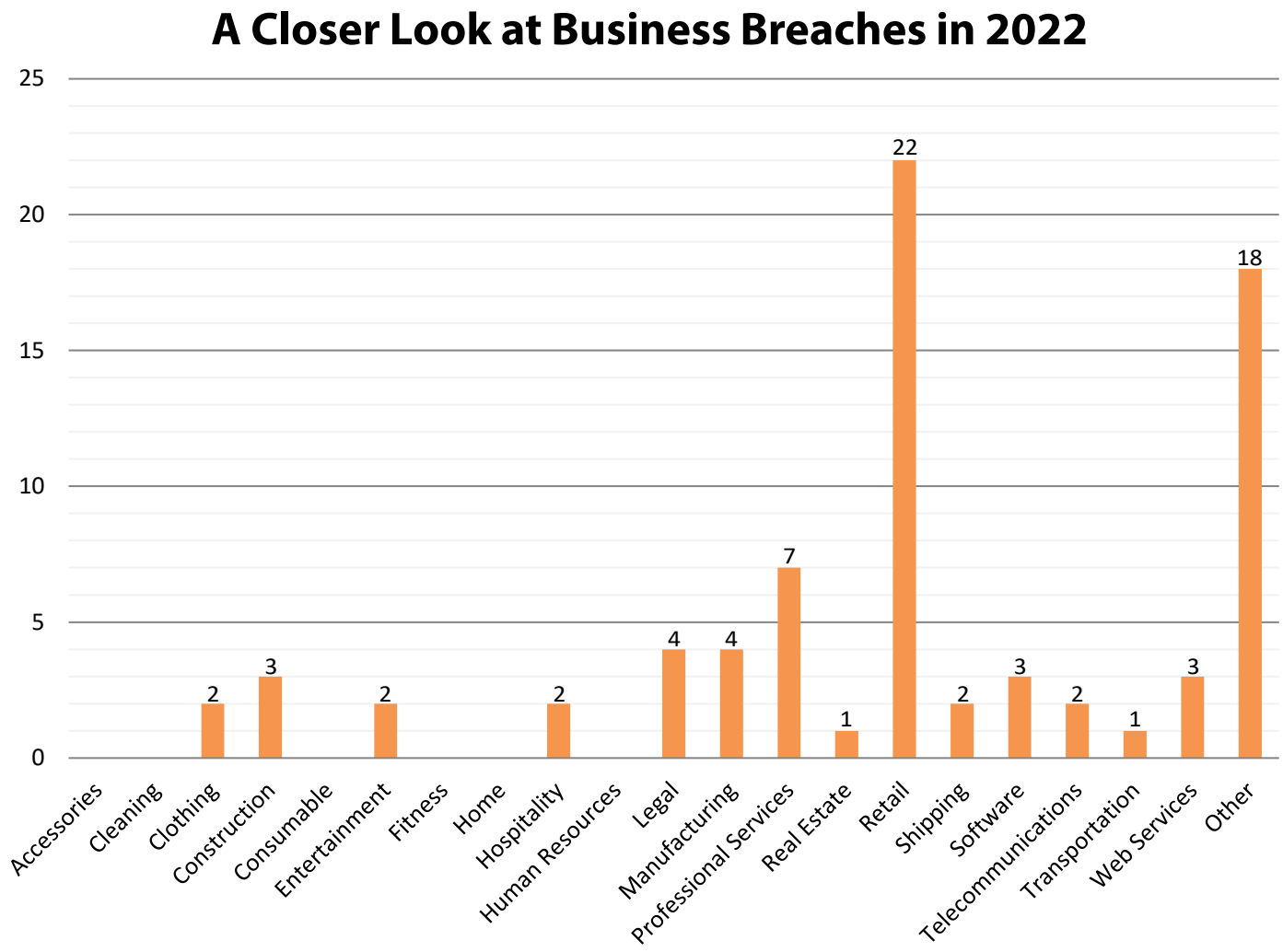
Government

Health Care

Non-Profit (NPO) & Charitable Organizations

The business category includes 23 sub-categories, including retail, manufacturing, transportation, construction, hospitality, and software.[3]

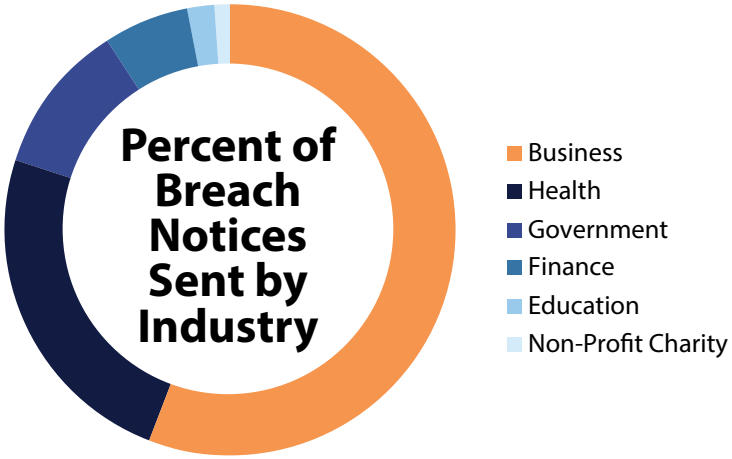
For a seventh straight year, the majority of breaches reported in 2022 came from organizations categorized as businesses, which accounted for 51% (76) of all breaches, and 57% (2,592,000) of all affected Washingtonians. Cyberattacks account for 75% of business data breaches. Of these, ransomware attacks and malware caused approximately half.

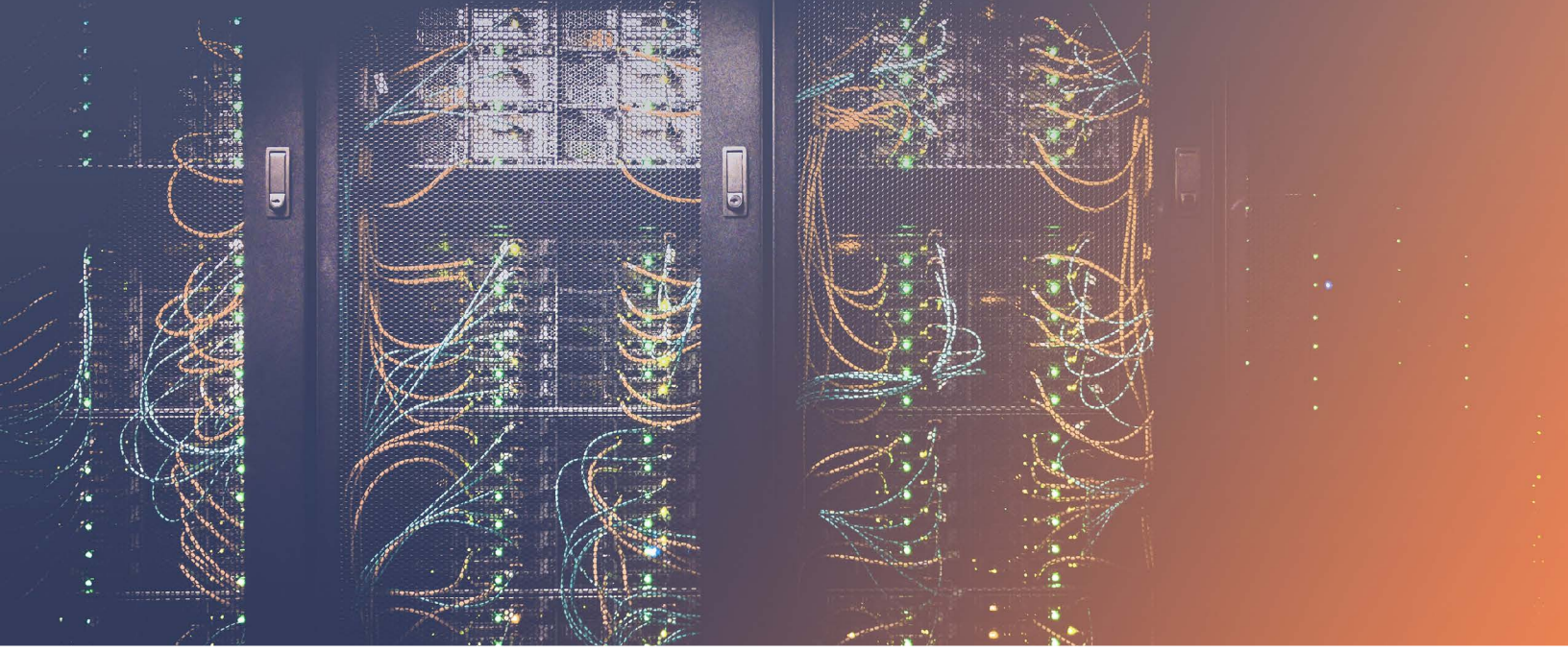


Retail (28.9%) and Professional Services (9.2%) sub-categories represented the most common types of businesses to be breached (except "Other"), together representing more than a third of all breaches reported by businesses.

Health organizations accounted for 21% (32 of 150) of breaches and 24% (1,070,000) of all Washingtonians affected.

Government entities accounted for 5% (7 of 150) of the breaches. Those breaches had an outsized impact, however, resulting in 11% (490,000) of the notices sent to Washingtonians this year. Lastly, after a horrendous 2021 for Non-Profit and Charity organizations driven by the breach of cloud-computing provider Blackbaud, breaches affecting NPOs sharply declined only accounting for 3% (5 of 150) of breaches, and 1% (25,000) of impacted Washingtonians in 2022.





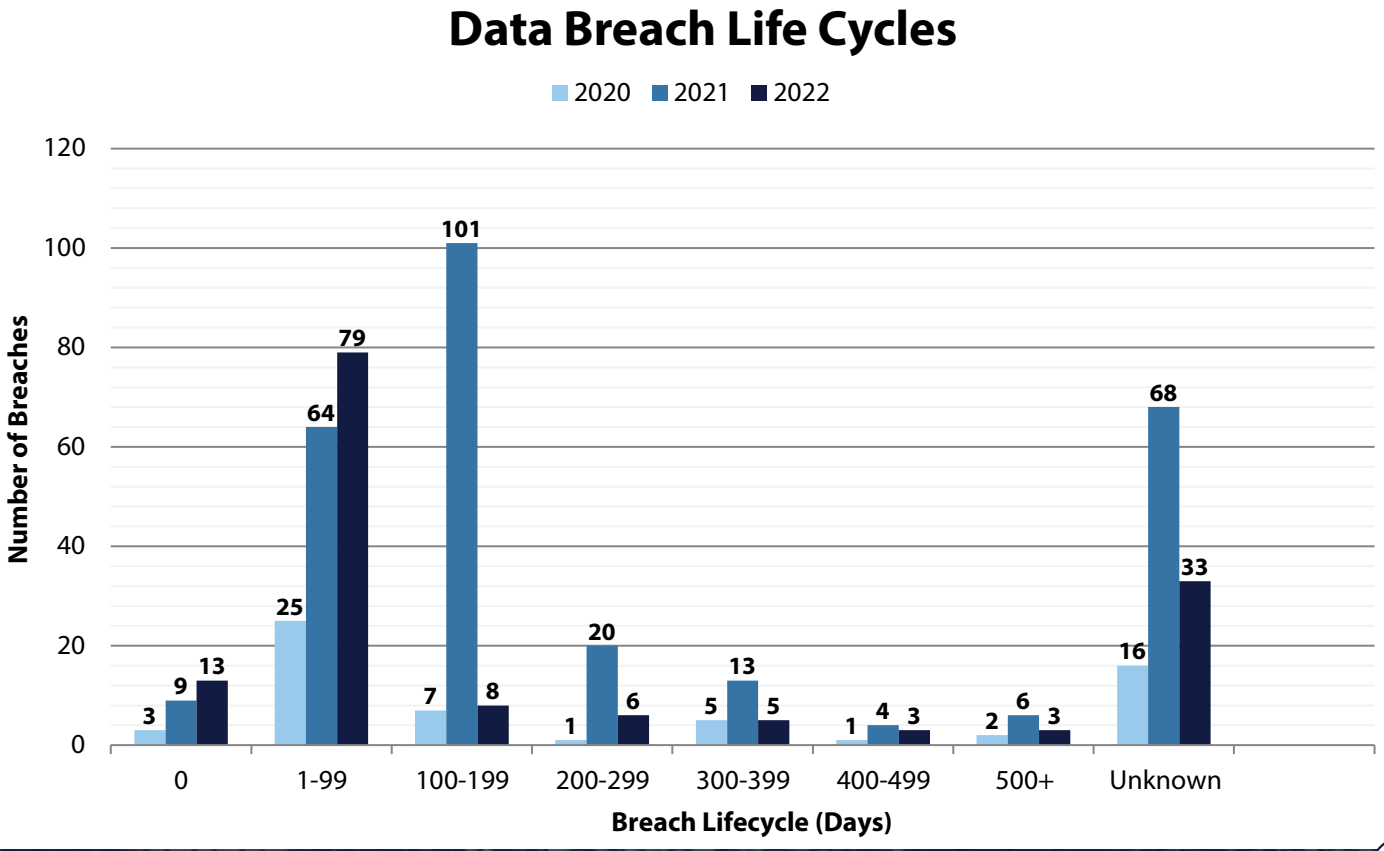
Time to Resolve Data Breaches

What is a Data Breach "Life Cycle"?

Resolution of a breach involves two steps:

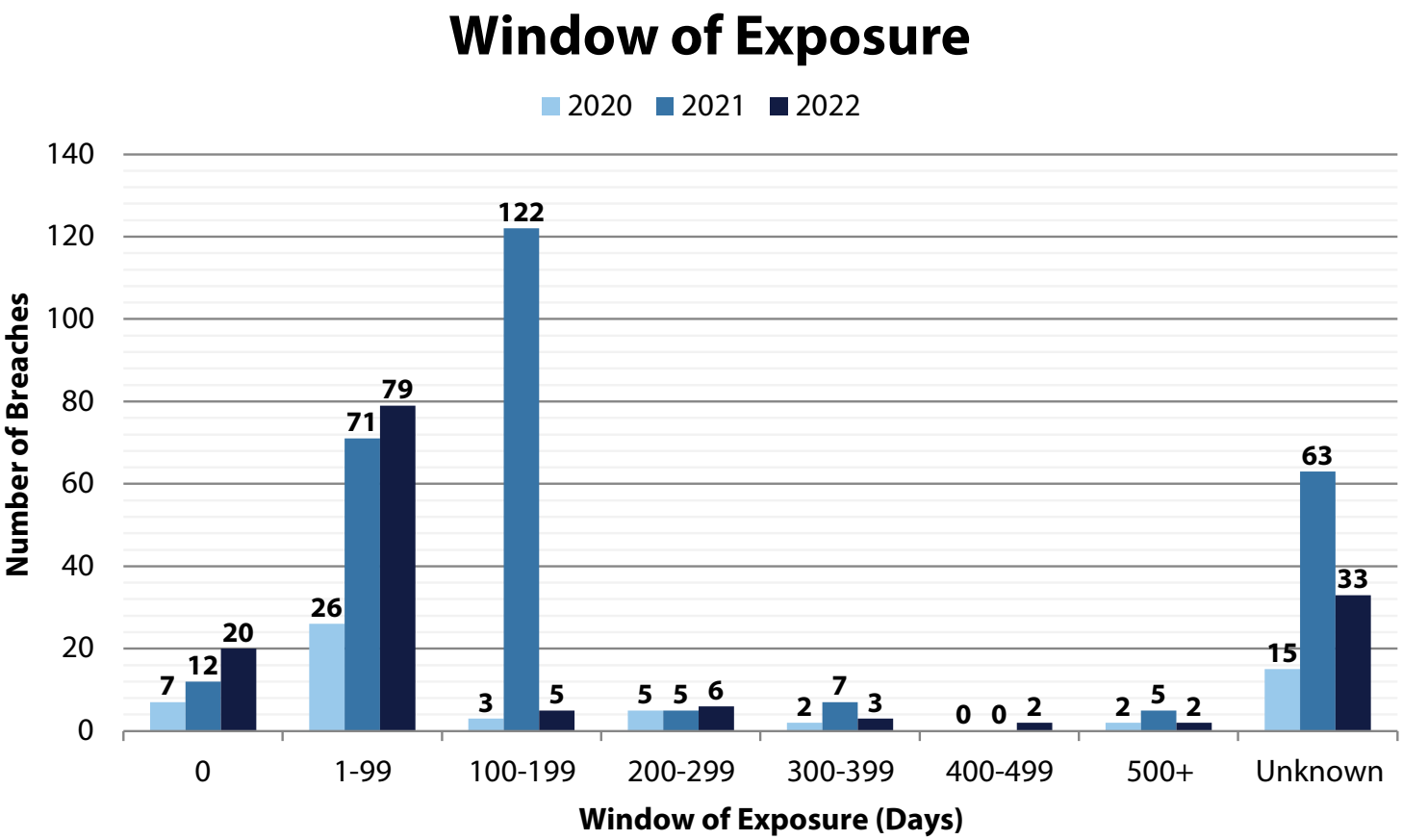
1. Identification of the breach; and
2. Subsequent containment of the breach.

This report defines "identification" as the number of days that pass between the start of the breach and its discovery by the affected organization. "Containment" is the number of days that pass between discovering the breach and restoring the integrity of the data system. The sum of these two measurements represents the "life cycle" of a breach.



What is a "Window of Exposure?"

The "window of exposure" is the period of time when personal information remains exposed to unauthorized individuals before breached organizations secure their systems.



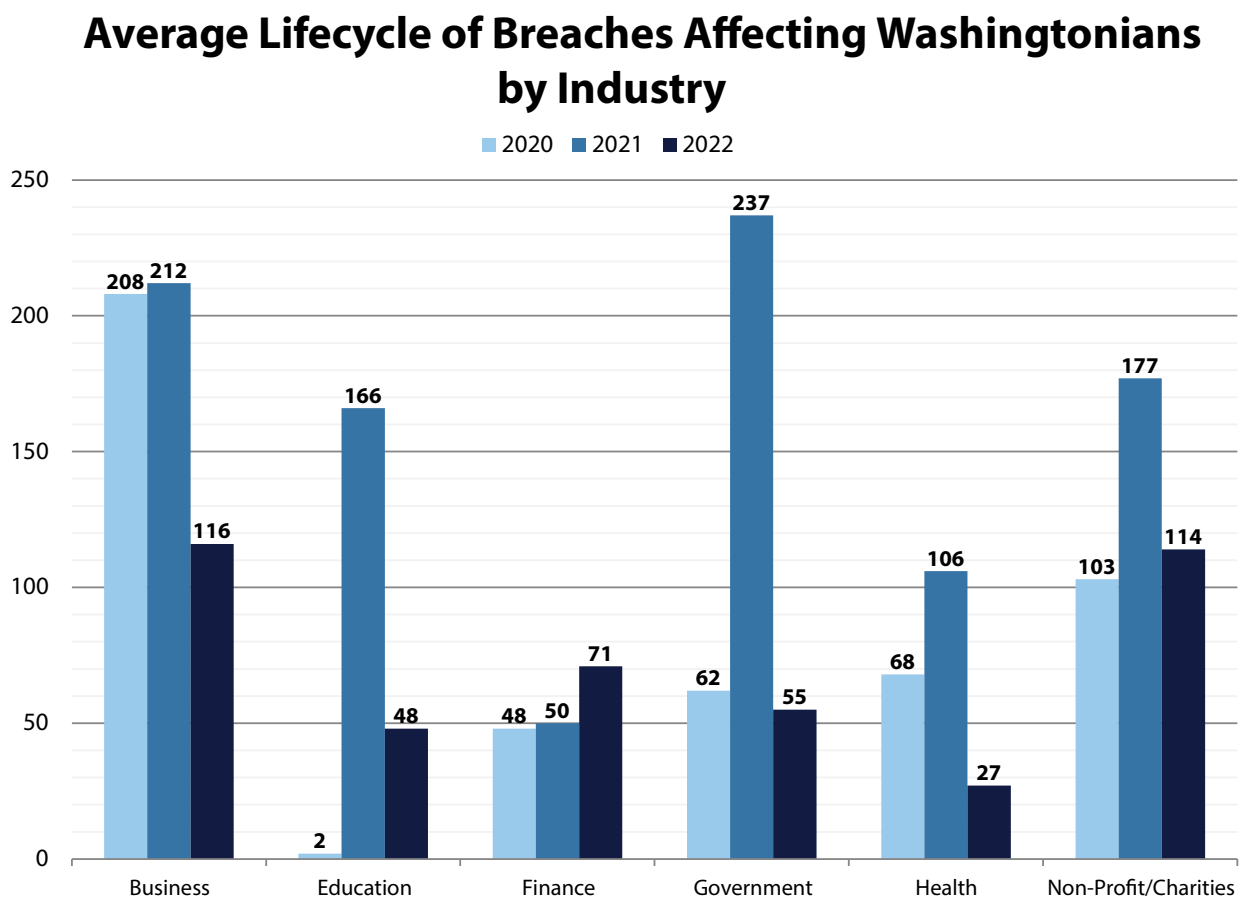
This year both the window of exposure and life cycle of a breach was shorter than 100 days for the majority of data breaches.

Case Example:

American Financial Resources, Inc. (AFR Inc.) reported a breach on March 11, 2022. Employees at AFR Inc. noticed suspicious activity on their network, and after an investigation, determined that sensitive data had been accessed without authorization. AFR Inc. determined that this unauthorized access occurred between December 6 and December 20 of 2020. This represents a window of exposure of approximately 14 days.

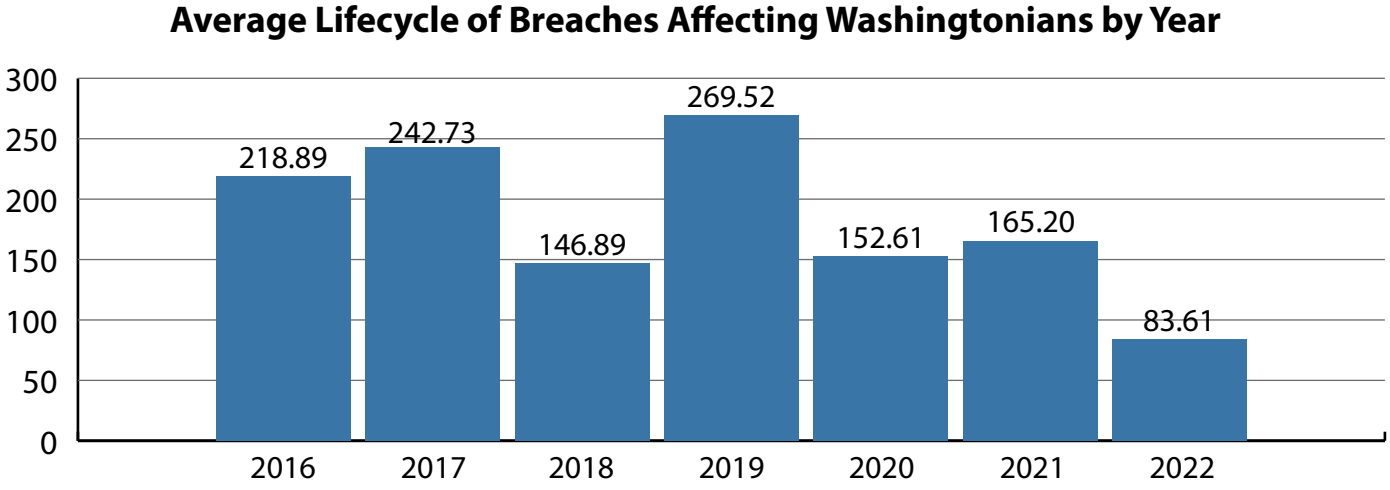
However, AFR Inc. did not notice the suspicious activity on their network until December 20, 2021 – a full year (365 days) after the breach began. As a result, the life cycle of this breach (379 days) was longer than the window of exposure (14 days). Breaches with long life cycles are of particular concern because they leave consumers uninformed of the risk to their information for a significant amount of time.

The Average Life Cycle of Breaches



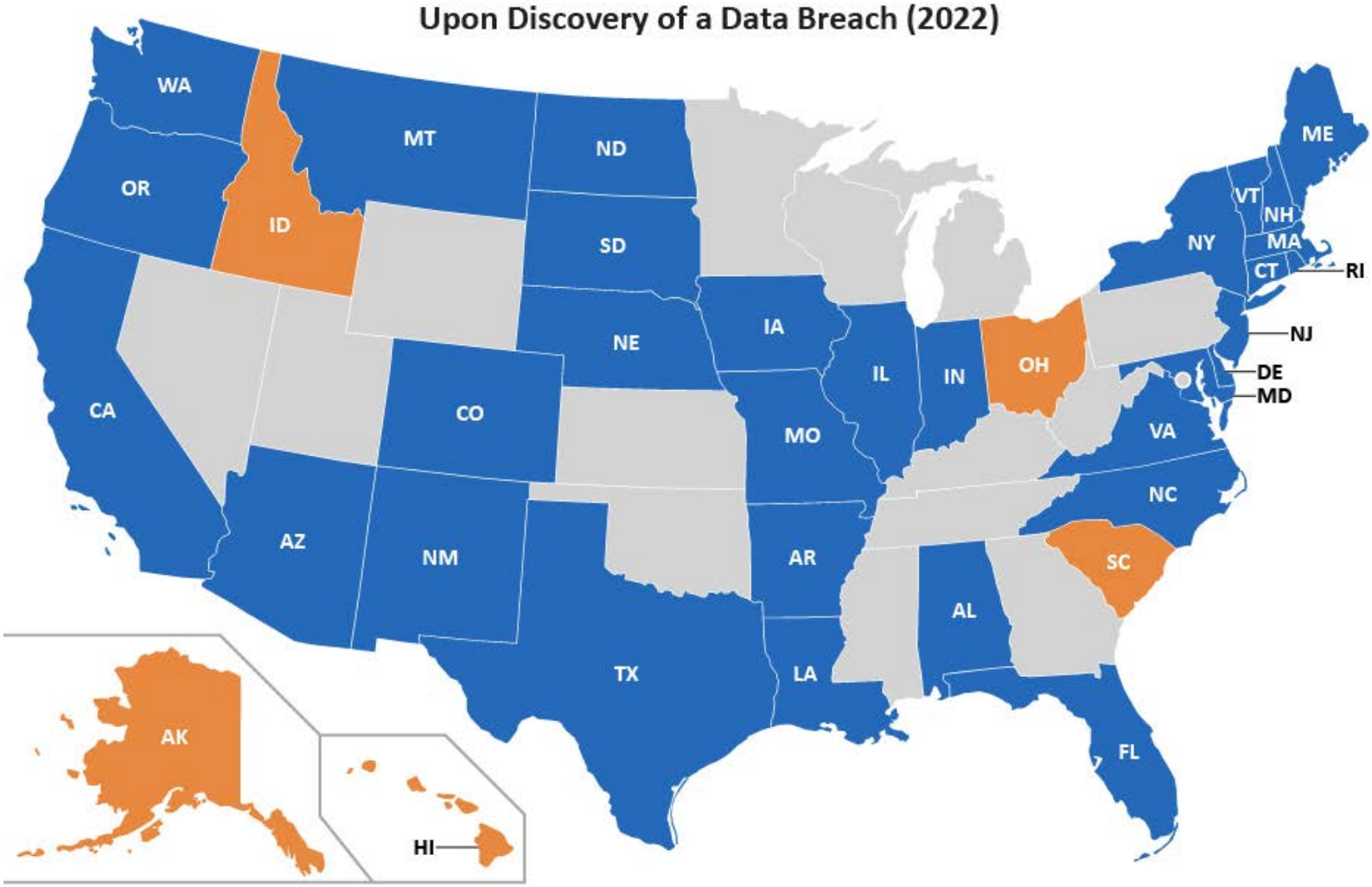
The average life cycle of a breach decreased significantly for almost all industries. According to the Ponemon Report, organizations that resolved data breaches in fewer than 200 days saved, on average, $1.12 million per breach compared to their counterparts who took more than 200 days.[4] Notably, the Ponemon Report also states that in 2022, the global average life cycle of a breach across all industries lasted 277 days, down from 287 days in 2021. On average, breaches reported to the AGO in 2022 had a life cycle of 84 days, a 49% decrease from 2021 (165 days).

This is the first year since tracking began in 2016 that the average breach life cycle fell below 100 days. This is an encouraging sign, and may indicate that organizations are committing more time and resources towards discovering and resolving breaches quickly. More data is necessary to determine if this is an aberration or the start of a positive trend, but it is certainly a welcome change compared to 2019, when the average life cycle of a breach in Washington was an all-time high of 270 days.



Washington's Data Breach Notification Law: The Strongest in the Country

States Requiring Notification of State Attorney General Upon Discovery of a Data Breach (2022)



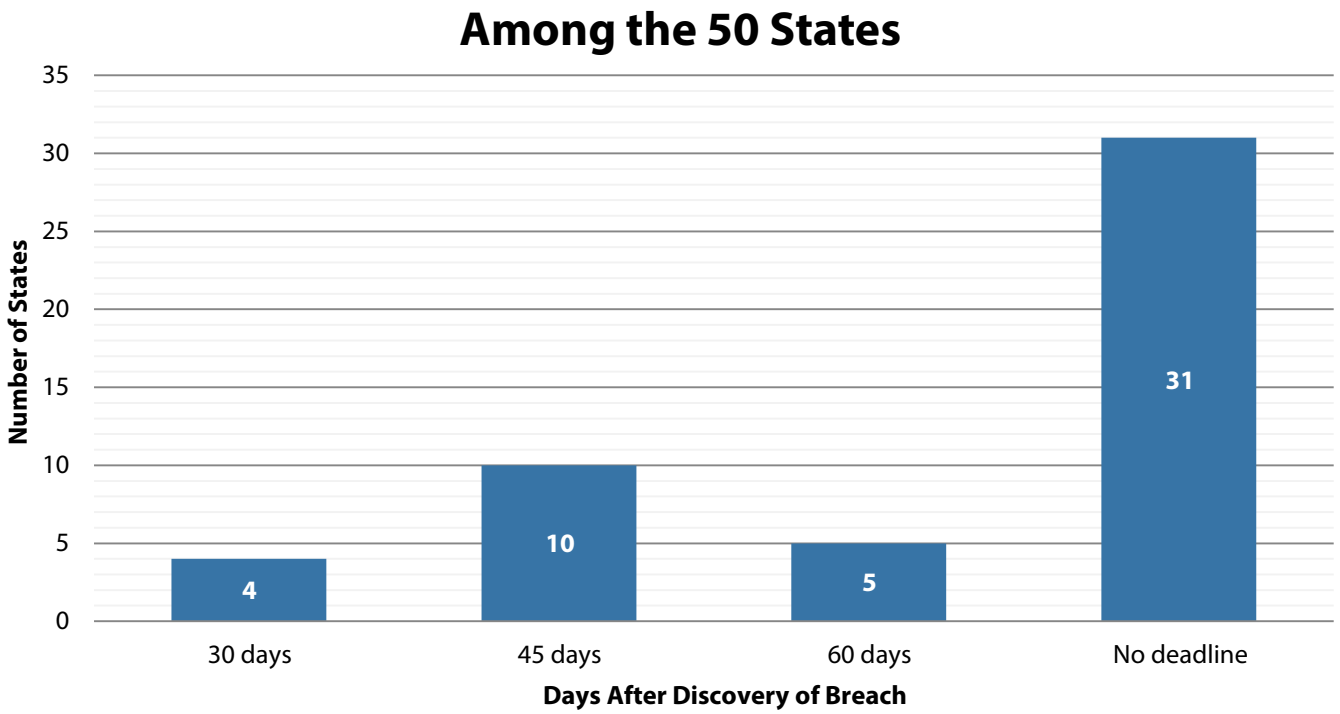
*States in orange only require notification to the Attorney General under special circumstances (e.g. Idaho only requires notice from public agencies), and/or require notification to a state agency that is not the Attorney General (e.g. Hawaii requires notice to the Office of Consumer Protection).

Washington Compared to Other States

All 50 states have laws requiring private or governmental entities to notify individuals when a data breach occurs.[6]

In all 50 states, notification of individuals is not required if the information compromised was encrypted, redacted, or otherwise unreadable. However, in 22 states, including Washington, notification is required when an encryption key or security credential that could render the personal information readable or usable is included in the breach, with the encrypted information.[7]

In 36 states, including Washington, entities experiencing a breach must notify the Attorney General or another state agency.[8] However, the timing, trigger, and scope of the notice varies from state to state. In Idaho, for example, if a public agency experiences a breach, it must provide notice to the Attorney General within 24 hours.[9] In Iowa, a breached entity is required to provide notice to the Director of the Consumer Protection Division at the AGO if it affects more than 500 Iowa residents, and must do so within 5 days of providing notice to consumers.[10] Unlike Washington, however, neither state has an explicit deadline to notify consumers for breaches affecting private entities.



Washington is one of 19 states that require a hard deadline for reporting breaches to consumers.[11] As of September 2021, Washington and three other states, Florida, Colorado, and Maine, require breached organizations to notify consumers within 30 days– the shortest, and, consequently, most protective deadline in the country.

Most states with a deadline, including Washington, trigger the timeline upon discovery of a breach of personal information and require notification "without unreasonable delay...unless the delay is at the request of law enforcement...."[12]

How Other States Define Personal Information

All 50 states adopted the same general definition of personal information (PI):

1. The first name or first initial and last name of an individual; and

2. One or more of the following data elements:
    a. Full Social Security number;
    b. Driver's license number or state-issued identification card number;
    c. Account, credit card, or debit card number in combination with any security code, access code, PIN, or password needed to access an account.

However, many states include additional data elements in their general definition of PI, including Washington. There are still a few elements included in various other states' laws that are not covered by Washington law, including individual tax ID numbers, tribal ID numbers, birth or marriage certificates, DNA profile, and mother's maiden name. Of these remaining elements, tax ID numbers appear the most, showing up in the data breach notice laws of eleven other states. The most recent state to add tax ID numbers to their statute was Connecticut, effective October 1, 2021.

Data Element	States With That Element in Their Definition of PI
Date of Birth	North Dakota, ***Washington***
Electronic Signature	Arizona, Iowa, Missouri, North Carolina, North Dakota, ***Washington***
Student ID Number	Colorado, New Hampshire, ***Washington***
Military ID Number	Alabama, California, Colorado, Connecticut, Florida, Maryland, Vermont, Virginia, ***Washington***, Wyoming
Passport ID Number	Alabama, Arizona, California, Colorado, Connecticut, Delaware, Florida, Louisiana, Maryland, North Carolina, Oregon, Vermont, Virginia, ***Washington***
Health insurance policy number	Alabama, Arizona, California, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Missouri, Nevada, North Dakota, Oregon, Rhode Island, Virginia, ***Washington***, Wyoming
Medical/Health information	Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Missouri, Montana, New Hampshire, North Dakota, Oregon, Rhode Island, South Dakota, Texas, Vermont, Virginia, ***Washington***, Wyoming
Biometric Data	Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Illinois, Iowa, Louisiana, Maryland, Nebraska, New Mexico, New York, North Carolina, Oregon, South Dakota, Vermont, ***Washington***, Wisconsin, Wyoming
Username and password	Alabama, Arizona, California, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Nebraska, Nevada, New Jersey, New York, Oregon, South Dakota, ***Washington***, Wyoming
Email address and password	Alabama, Arizona, California, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Nebraska, Nevada, New Jersey, New York, Rhode Island, South Dakota, ***Washington***, Wyoming
Individual Taxpayer ID number	Alabama, Arizona, California, Connecticut, Delaware, Maryland, Montana, North Carolina, Vermont, Virginia, Wyoming

In addition to these individual elements, there are also differences from state to state in how each element triggers the notification statute. For example, in Colorado's law, financial information, like account, debit, or credit card numbers in combination with passwords or security codes, is not required to be in combination with an individual's name to trigger the notification statute.[13]

Massachusetts' law, conversely, requires names to be part of the breach of financial information to trigger notice, but not passwords or security codes.[14] Nuances like this exist for other data elements as well, such as Indiana's notification law, which triggers if an individual's Social Security number is breached, even if the name of the associated individual is not.[15]
At the time of publication, Washington's law stands out by defining more elements of personal information than any other state (15). This, in combination with being one of four states with the shortest deadline for consumer notice (30 days), and one of the only states that continues to track and publish figures on data breach incidents and laws through the Attorney General's annual Data Breach Report, makes Washington a clear leader on the issue of Data Breaches nationally.

For a detailed breakdown of Washington's current notification statute see: Washington's Data Breach & Data Security Laws in the Appendix on page 25.

Recommendations

Our office recommends legislators consider taking the following actions to protect Washingtonians' data and privacy:

1. **Pass legislation to protect consumers' private health data**

A variety of entities, including apps, websites, and mobile devices, collect personal health data but are not subject to the Health Insurance Portability and Accountability Act (HIPAA). HIPAA covers some entities that collect personal health data—health plans, most health care providers, and health care clearinghouses—but does not cover the data itself.[16] This means that the privacy protections provided by HIPAA do not apply to employers, school districts, law enforcement, and health apps such as period tracking, activity tracking, or other apps used to manage health conditions.

The limited scope of HIPAA means that data entered into, or collected by, consumer health apps, such as pregnancy and fertility trackers, and personal fitness and exercise apps, may be shared with third parties or sold according to the terms and conditions for use of the apps. Under current law, Washingtonians' health data is left vulnerable to be used by advertisers or shared with anti-choice groups. For example:

- Period tracking apps can sell sensitive information about a woman's late period or miscarriage to data brokers. Data brokers can link that information to her data profile, which is essentially for sale on the open market. Law enforcement from states with strict anti-abortion laws or anti-choice advocacy groups can purchase that data profile and use that information to prosecute women who had an abortion or miscarriage in another state.
- Pregnant individuals sometimes contact or visit crisis pregnancy centers looking for reproductive health care services, only to find that they cannot receive an abortion at that facility. But while they are there, the crisis pregnancy center can collect and share the woman's sensitive data with anti-abortion groups who can then target the woman with pro-life messaging and political ads.
- Digital advertising firms can set up geofencing around health care facilities that trip when a person brings their cell phone or mobile device across the barrier. The individual can be bombarded with text messages and advertisements urging them not to seek reproductive or gender-affirming care.

The Washington Consumer Health Privacy Act, Attorney-General request legislation sponsored by Senator Manka Dhingra and Representative Vandana Slatter, will require that any entity that collects consumer health data must:

(1) Create and maintain a privacy policy specific to consumer health data;
(2) Provide consumers the right to request that the entity delete their health data;
(3) Provide consumers the right to opt-out of the collection and sharing of their health data and prohibit the collection or sharing of consumer health data without consent; and
(4) Fully prohibit the sale of consumer health data to third parties.

2. **Enact legislation to enable consumers to better control their personal data and reduce the risk of losing information to a data breach by requiring organizations to recognize and honor opt-out preference signals.**

Consumers who want to limit the sharing of their personal information by businesses they interact with online can use an opt-out preference signal. An opt-out preference signal, also sometimes referred to as a "Global Opt-Out" signal, is a digital signal sent with a consumer's consent automatically by a platform, technology, or mechanism to a business indicating the consumer's intent to opt-out of the business' sharing of the consumer's personal information. A consumer who selects an opt-out option in their browser will send any website that they visit in that browser an automatic signal that they are opting-out of any sharing of their personal information. An example of an existing opt-out preference signal is the Global Privacy Control.[17]

A global opt-out signal gives consumers the power to assert that they do not want their information shared without requiring consumers to:

(a) Reach out directly to every individual website they visit, or
(b) Identify every vendor used by a particular business that processes their personal information – for example, vendors used to process credit card payments.

In order to be effective, businesses must honor opt-out signals. If lawmakers require that opt-out signals are honored, consumers will gain a powerful tool to control their data, and reduce the risk that a breach will expose their personal information.

This reform will reduce the impact of data breaches. Both the California Consumer Protection Act (CCPA) and Europe's Global Data Protection Regulation (GDPR) require businesses to honor consumers' opt-out preference signals. Washington residents deserve these same protections and autonomy over how, and whether, their data is shared on the internet.

3. **Make data breach notices accessible for Washingtonians who do not speak English as their primary language.**

According to the Office of Financial Management (OFM), 20% of households in Washington State speak a language other than English.[18] English is spoken less than "very well" in 7.6% of Washington households. Despite this, no data breach notices provided to our office in 2022 included information about where to find the notice in another language.

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 one or more of the following policy proposals:

- 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;
- Require data breach notices be provided in any language that a breached entity advertises their products or services in; or
- Fund an interpreter service explicitly aimed at supporting Washingtonians with limited English proficiency who were impacted by a data breach (i.e. data breach notice interpretation, contacting and working with credit agencies).

4. **Expand the definition of "personal information" in RCW 19.255.005 to include (a) full name in combination with a redacted Social Security Number that still exposes the last four digits of the number 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 failed to make the same change to breaches of businesses. 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." In 2018, Washington State was home to just over 1.1 million foreign born individuals, representing approximately 15% of the state's population.[19] According to the American Immigration Council, in 2018, foreign-born households in Washington contributed an estimated $3.9 billion in state and local taxes in 2018, and foreign-born business owners generated $2.3 billion in business income.[20] Our state's foreign-born residents deserve the same protection that those with Social Security numbers have.

5. **Require more transparency from data brokers and data collectors so Washingtonians know more about the consumer information these entities control.**

Policymakers must urgently recognize that privacy regulations have lagged significantly behind the pace of technology and business practices. Nearly every app and website collects personal information from consumers. It is extraordinarily difficult for consumers to know how much of their data, and what data, is being processed, by whom, and for what purpose. Consequently, Washingtonians generally do not have access to the information necessary to reduce the risk of having their data exposed in a data breach. To address this, the Legislature should pass legislation to require data brokers and controllers to report annually to individual consumers, via physical or electronic mail, what information they presently hold, and what information they have shared or sold, and to whom, in language that is clear and accessible. Additionally, lawmakers should require data brokers to be licensed by the state and provide regulators with information about the consumer data it processes its policies for allowing consumers to control their data or opt-out of data processing, and the data security measures it uses.

Consumer Privacy Rights Legislation

The AGO strongly supports improved data privacy protections. For years, however, the Attorney General's Office successfully opposed weak, ineffective data privacy legislation from passing the Washington Legislature. The Attorney General's Office supported, with some qualifications, federal data privacy legislation proposed by Senator Maria Cantwell.

Below is a side-by-side crosswalk comparing the Consumer Online Privacy Rights Act, S. 3195, sponsored by Senator Cantwell, the American Data Privacy and Protection Act, H.R. 8152, sponsored by Representatives Frank Pallone and Cathy McMorris Rodgers, and the Washington Data Privacy Act, SB 5062. This crosswalk demonstrates the comparative weakness of legislation offered in Washington.

Until the Legislature adopts a strong data privacy law, the AGO will continue to use its existing tools under the Consumer Protection Act to uphold Washingtonians' data privacy.

KEY (Policy Strength)		
Weak	**Moderate**	**Strong**
The legislation does not address the policy issue, or the proposed policy adversely affects consumers' interests.	The legislation addresses the policy issue, and somewhat benefits the consumer.	The legislation directly addresses a policy issue, and centers consumers' interests above other considerations.

	S. 3195	H.R. 8152	SB 5062
Government Enforcement	**STRONG** Federal Trade Commission enforcement + State Attorney General enforcement (no right to cure or other limitations) (Sec 301(a)-(b))	**MODERATE** Federal Trade Commission enforcement + State Attorney General enforcement in federal court (no right to cure) (Sec. 401 & 402)	**WEAK** Limited AG-enforcement w/ right to cure (Sec. 112)
Enforcement by Individuals	**STRONG** Individuals can seek an amount not less than $100 and not greater than $1,000 per violation per day or actual damages, whichever is greater; punitive damages; reasonable attorney's fees; and any other relief that the court determines appropriate. (Sec. 301(c))	**MODERATE** Private right of action allowed after 2-year delay. Class actions explicitly allowed. Lawsuits can seek actual damages, injunctive relief, and reasonable attorneys' fees (subject to limited right to cure).	**WEAK** Private rights of action explicitly prohibited (Sec. 111)
Preemption	**MODERATE** Preempts state laws, but notes that state laws "shall not be considered in direct conflict if it affords a greater level of protection" (Sec. 302)	**WEAK** Preempts state laws (Sec. 404(b))	**N/A**
Algorithmic Discrimination	**STRONG** Bans algorithmic discrimination. (Sec 108(b))	**STRONG** Bans algorithmic discrimination. (Sec. 207)	**WEAK** Does not address algorithmic discrimination.
Privacy Policy	**STRONG** Requires clear, conspicuous privacy policy. (Sec 102)	**STRONG** Requires clear, conspicuous privacy policy. (Sec. 202)	**WEAK** Does not require a privacy policy.
Loopholes	**STRONG** No broad data exemptions	**WEAK** Exemption for data used to "conduct internal research or analytics to improve products and services" (Sec. 101(b)) Certain exemptions for service providers (Sec. 2(9)(C))	**WEAK** Exempts all data controlled by non-profits for 4-years after effective date. Exempts data controlled by entities subject to HIPAA.
Whistleblower Protections	**STRONG** Includes whistleblower protections. (Sec. 204)	**WEAK** No whistleblower protections.	**WEAK** No whistleblower protections.

Resources for Individuals Affected by a Data Breach or Identity Theft

While there are steps you can take to protect yourself from identity theft, there is no foolproof way to ensure that your information is safe. If you receive a breach notification or believe that you may be a victim of identity theft, please visit the AGO's website at http://www.atg.wa.gov/GUARDIT.ASPX for help.

https://identitytheft.gov, provided by the U.S. Federal Trade Commission (FTC), is also a valuable resource for victims – or potential victims – of identity theft. If you suspect you are the victim of identity theft:

1. Call the companies where the fraud may have occurred;
2. Work with at least one of the credit bureaus (Experian, TransUnion, and Equifax) to check your credit report for suspicious activity and to place a fraud alert or credit freeze on your credit report;
3. Report the identity theft to the FTC at IdentityTheft.gov;
4. File a report with your local police department;
5. Send a copy of the police report to the three major credit bureaus; and
6. Ask businesses to provide you with information about transactions made in your name. A template for a letter you can complete and send to businesses to request records is available on the Attorney General's Office website at: https://www.atg.wa.gov/db-letter.

Resources for Businesses

Any organization entrusted with individuals' information is potentially susceptible to a data breach. The AGO provides resources for businesses to secure the data they hold and protect against data breaches. The office also provides information explaining the laws regarding data breaches and notifications. These resources are available at https://www.atg.wa.gov/identity-theft-and-privacy-guide-businesses.

You can find a FAQ providing specific information about the March 2020 update to our state's data breach notification laws here: https://www.atg.wa.gov/hb1071-faq.

Basic steps businesses can take to protect consumers' personal information include:

1. 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;
2. Minimize the amount of information that you collect and retain. Delete any information that is no longer necessary. Also, consider reviewing RCW 19.215, "Disposal of Personal Information" for more details;
3. Develop policies for the collection, encryption, and use of "personal information;" and
4. Prepare ahead of time. 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. Page 59 of the 2021 Ponemon Report provides more detail on these steps, and others. You can find the report for download here: https://www.ibm.com/security/data-breach.

Washington's Data Breach Notification Laws

Under RCW 19.255.010 and RCW 42.56.590, businesses and public agencies are required to notify affected individuals when a data breach occurs. The AGO must also receive notice when a data breach requires notification of more than 500 Washington residents. The notice to consumers and the AGO must be provided without unreasonable delay, no more than 30 days after the breach was discovered. According to state law, notification is required when a business or public agency experiences a breach of personal information if:

- The breach is reasonably likely to subject an individual to a risk of harm;
- The information accessed during a breach was not secured; or
- The confidential process, encryption key, or other means to decipher the secured information was acquired.

The notice provided to the AGO must include:

- The total number of Washingtonians affected;
- A list of the types of personal information affected;
- The time frame of exposure;
- A summary of steps taken to contain the breach; and
- A copy of the breach notification sent to affected consumers.

The updated law also requires breached entities to provide updates to the notice provided to the AGO if any of the required information is unknown at the time the notice is due.

A list of all data breach notices the AGO since 2015 is publically available at https://www.atg.wa.gov/data-breach-notifications.

Definition of Personal Information

Under Washington's notification laws "personal information" is defined as someone's first name or first initial and last name in combination with any of the following data elements:

- Social Security number;
- Driver's license number or Washington identification card number; or
- 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
- Student, military, or passport identification numbers; or
- Health insurance policy or identification numbers; or
- Full date of birth; or
- Private keys for electronic signature; or
- Medical information, including medical history, mental or physical condition, diagnoses, or treatment; or
- Biometric data.

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

Lastly, any username or email address in combination with a password or security questions and answers that would permit access to an online account is also personal information.

Also of note, SB 6187 slightly modifies the definition of personal information for breaches that occur at local and state agencies. Specifically, the bill modifies the definition of personal information in RCW 42.56.590 to include the last four digits of a SSN in combination with a consumer's name as a stand-alone element that will trigger the requirement for consumer notice. When the entity holding this personal information is covered by the Health Insurance Portability and Accountability Act (HIPAA) the entity must provide notification to the AGO of a breach. These entities are deemed to

comply with the timeliness of the notification requirement as long as they comply with the requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Identity and Financial Information Theft Laws

Under Washington's criminal law, improperly obtaining financial information is a Class C felony (RCW 9.35.010). It is illegal to obtain or seek to obtain financial information that a person is not authorized to have. The law also establishes the crime of identity theft, which focuses on financial information, as a Class B or C felony, depending on the damage caused (RCW 9.35.020). County prosecuting attorneys enforce this law.

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, 2022.

In 2021, our office was fortunate to have the time and resources to build 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. Already, this form has achieved more accurate and complete information 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 2021 increased from the 6,385,000 figure we reported last October, to an updated total of 6,507,000.

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."

Special Thanks

The completion of this report would not have been possible without the tremendous 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
Joe Kanada, Consumer Protection Division
Andrea Alegrett, Consumer Protection Division
Brionna Aho, Public Affairs
Beth Carlson, Public Affairs
Ian Couch, Public Affairs

Notes & Citations

1: Ponemon Institute. (2022, July). "2022 Cost of a Data Breach Report."

2: RCW 19.255.010, effective since March 2020.

3: The full list of business sub-categories includes: Accessories, Biotech, Cleaning, Clothing, Construction, Consumable, Cosmetic, Cryptocurrency, Entertainment, Fitness, Home, Hospitality, Human Resources, Legal, Manufacturing, Professional Services, Real Estate, Retail, Shipping, Software, Telecommunications, Transportation, and Web Services. We also use an "other" category to capture any businesses that do not fit into the above.

4: Ponemon Institute. (2022, July). "2022 Cost of a Data Breach Report."

5: Data for this map was derived from Perkins Coie. (2021, September). "Security Breach Notification Chart." Accessed August 2022, from https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

6: Perkins Coie. (2021, September). "Security Breach Notification Chart." Accessed August 2022, from https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

7: Ibid.

8: Ibid.

9: Idaho Code § 28-51-104 (2006); as amended (2010).

10: Iowa Code § 715C.1-2 (2008); as amended (2018).

11: Perkins Coie. (2021, September). "Security Breach Notification Chart." Accessed August 2022, from https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

12: RCW 19.255.010, effective since March 2020.

13: Colo. Rev. Stat. Ann. § 6-1-716 (2006); as amended (2018).

14: Mass. Gen. Law Ann. Ch. 93H, §§ 1 (2007).

15: Ind. Code Ann. §§ 24-4.9 et seq. (2006); as amended (2009).

16: U.S. Department of Health and Human Services. (2022, January 19). "Your Rights Under HIPAA." Accessed August 2022, from https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

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

18: 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.

19: 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#.

20: American Immigration Council. (2020, August 6). "Immigrants in Washington." Accessed August 2021, from https://www.americanimmigrationcouncil.org/sites/default/files/research/immigrants_in_washington.pdf.