WASHINGTON STATE ATTORNEY GENERAL'S OFFICE

2021

DATA BREACH REPORT

TABLE OF CONTENTS

LETTER FROM THE ATTORNEY GENERAL

October 2021

Dear Washingtonians,

This report represents the latest effort in my commitment to protect your data privacy.

This is the sixth annual Data Breach Report published by my office. We receive no funding for this report. The Legislature does not direct our office to produce this report. We provide this report as a public service because we believe that you are best able to safeguard your data when you are aware of the threats.

For this reason, I twice led successful initiatives to strengthen Washington's data breach notification laws. As a result, Washington now has one of the most — if not *the* most — robust Data Breach Notification laws in the country.

Data breaches are a significant ongoing threat to Washington residents, businesses, and agencies. In the last year, breached businesses and agencies sent **6.3 million notices to Washingtonians — by far the largest number of Washingtonians affected in a single year since we began tracking this data.**

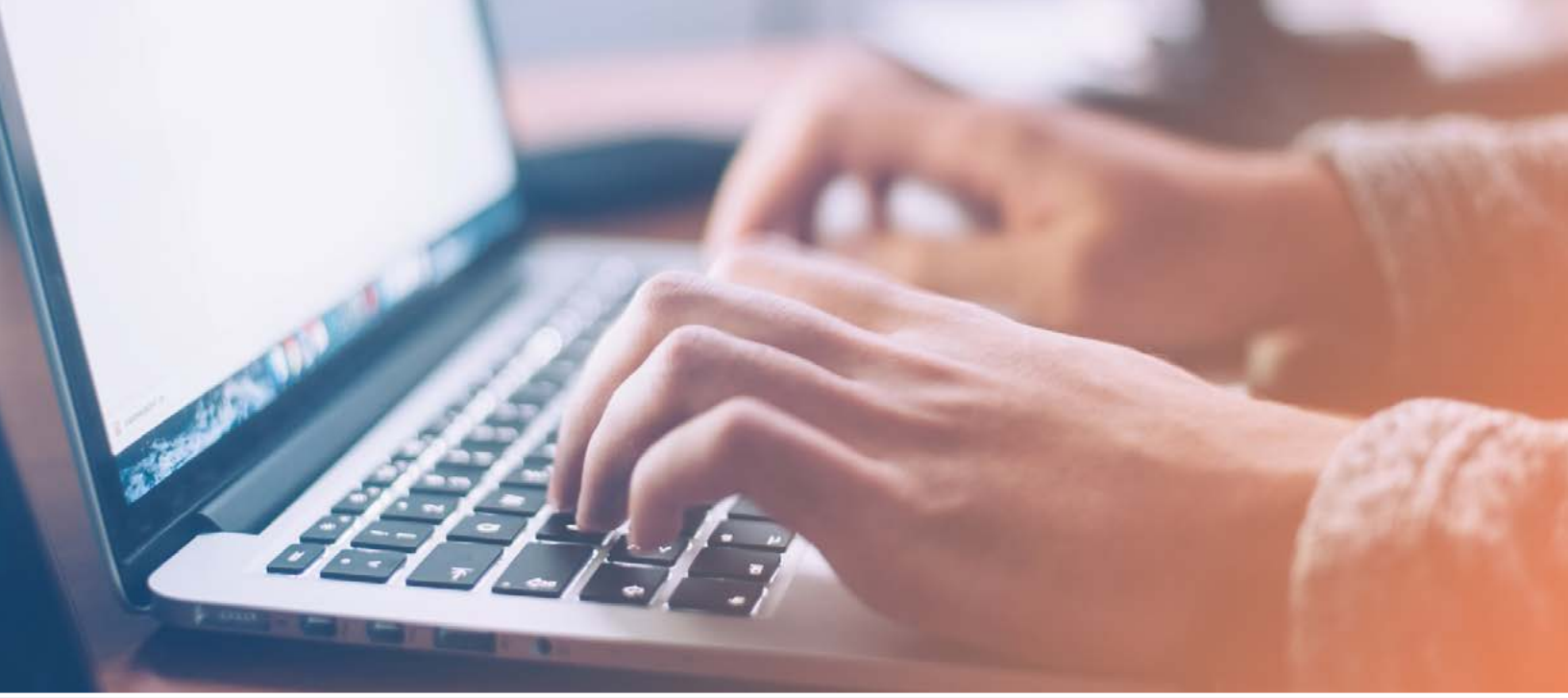
Additionally, my team recorded **a huge spike in ransomware incidents.** Ransomware — a type of cyberattack in which a cybercriminal uses malicious code to hold data hostage in hopes of receiving a ransom payment from the data holders — represents a growing and significant threat to your data and your business.

My office continues to initiate Consumer Protection Act cases against companies who experience data breaches because of lax security that falls short of industry standards. These cases have forced many companies to improve their security, with our office recovering more than $16 million for the State of Washington, which we have invested into future enforcement. **But often, you are in the best position to protect your business and your data.**

You will find resources and best practices for you and your business in this report. Moreover, we have included recommendations for lawmakers to strengthen Washington's laws. As long as I am the people's lawyer, I will continue fighting for your data security and online privacy.

Sincerely,

Bob Ferguson
Washington State Attorney General



Executive Summary

- **2021 set a new record for the highest number of data breach notices sent to Washingtonians (6.3 million).**
    - This represents approximately an 80% increase on the previous record of 3.5 million (2018).
    - Moreover, this is a nearly 500% increase over last year.
- **Businesses, agencies and other entities 280 reported to our office — also a new record.**
    - This represents about a 260% increase over the previous record of 78 (2017), and nearly five times last year's total of 60 breaches.
- **Cyberattacks and ransomware attacks spiked in 2021.**
    - Cyberattacks caused 87.5% of all reported data breaches — up from 63% in 2020.
    - 150 notices cited ransomware in 2021 — more than the last 5 years combined. A significant proportion of these refer to the ransomware breach of Blackbaud.
    - Ransomware attacks accounted for 61% of all cyberattacks (150 of 245) and more than half of all breaches (150 of 280).
- **2021 saw the first recorded mega breach since 2018.**
    - The cyberattack targeted Accellion, a company that specializes in file sharing technology, resulting in the exposure of files in the possession of the Washington State Auditor's Office. These files contained the personal information of approximately 1.3 million Washingtonians, including residents' names, Social Security numbers, dates of birth, bank account and routing numbers, addresses, and email.
    - This is the third reported mega breach since 2016.

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 Attorney General's Office 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 year's Data Breach Report is the first to include a full year of data since the 2019 law went into effect. It is based on data breach notifications received by the Attorney General's Office between July 24, 2020 and July 23, 2021 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 24.

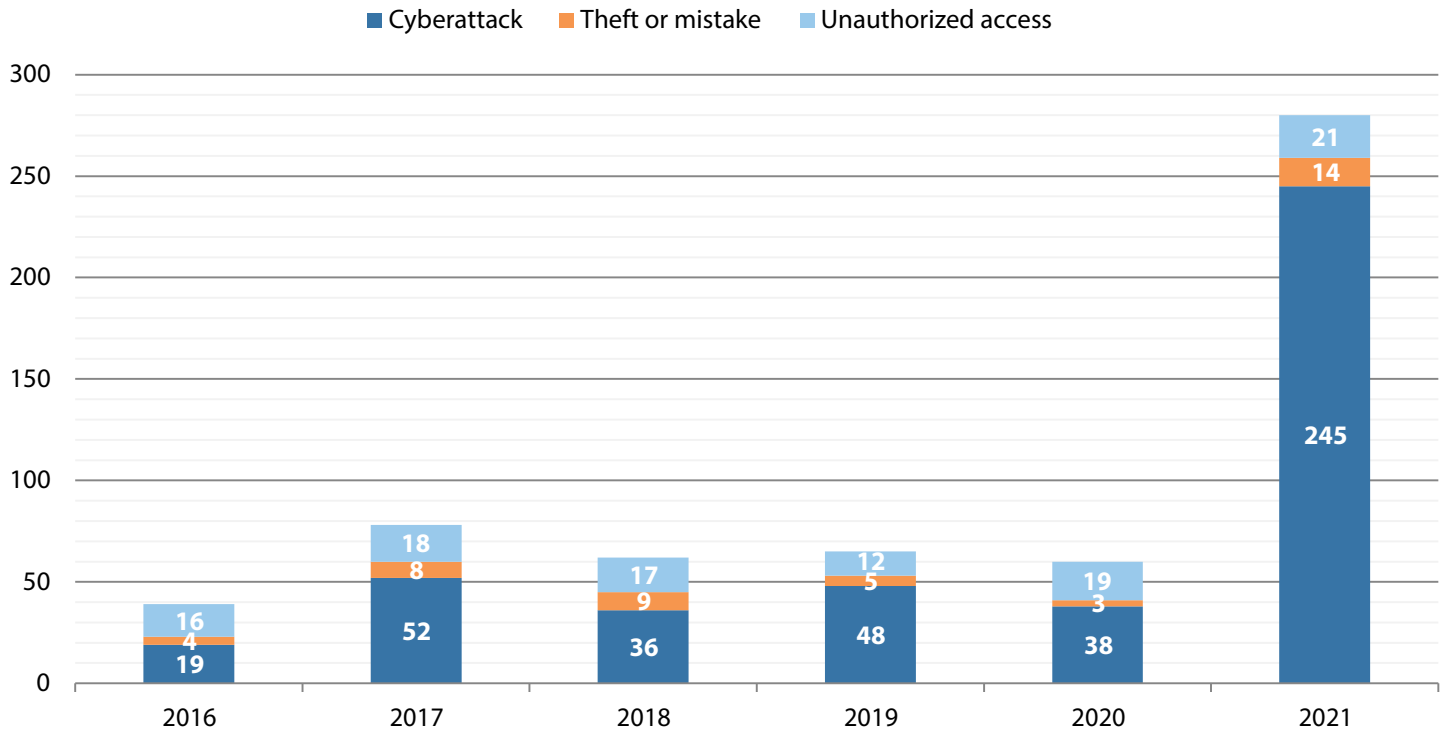
Recommendations

While our state's data breach notification law is one of the most robust in the country, policymakers can continue strengthening these protections for Washington residents. The Attorney General's Office recommends that policymakers:

1. Amend the definition of "personal information" (PI) in RCW 19.255.005 to include redacted Social Security numbers (SSNs) that display the last four digits of a Social Security number.
    - SB 6187 amended the definition of RCW 42.56.590 (covering government agencies) to include redacted SSNs, and this definition should extend to RCW 19.255.005 (covering businesses) as well.
2. Amend the definition of "personal information" to include Individual Tax Identification numbers (ITINs).
    - ITINs are a unique identifier assigned by the IRS to foreign-born individuals that are equivalent in sensitivity to a Social Security number. Our state's foreign-born residents deserve equal protection. At the time of writing, 10 states include ITINs in their definition of PI.

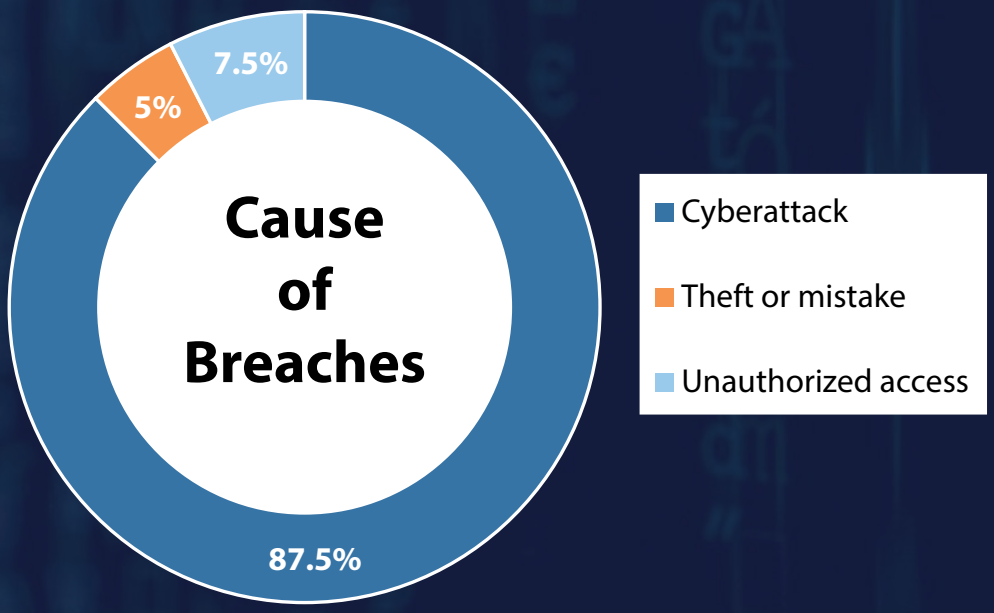
Causes of Data Breaches

Total Number of Data Breaches by Cause



Our office sorts the causes of data breaches into three broad categories:

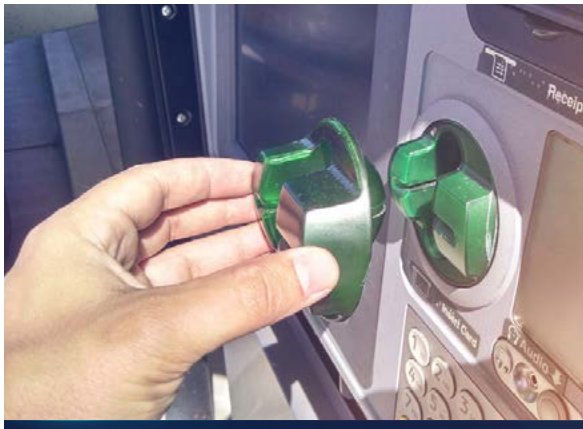
1. Cyberattack: A third party deliberately attempts to access secured data, such as information stored on a server, using cyber technology. The attack can use a skimmer, spyware, phishing email, or similar means of accessing secure data remotely.
2. Theft or mistake: The mistaken loss of information, such as a clerical error that sent W-2 information to an unintended recipient, or the inadvertent theft of information, such a stolen 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

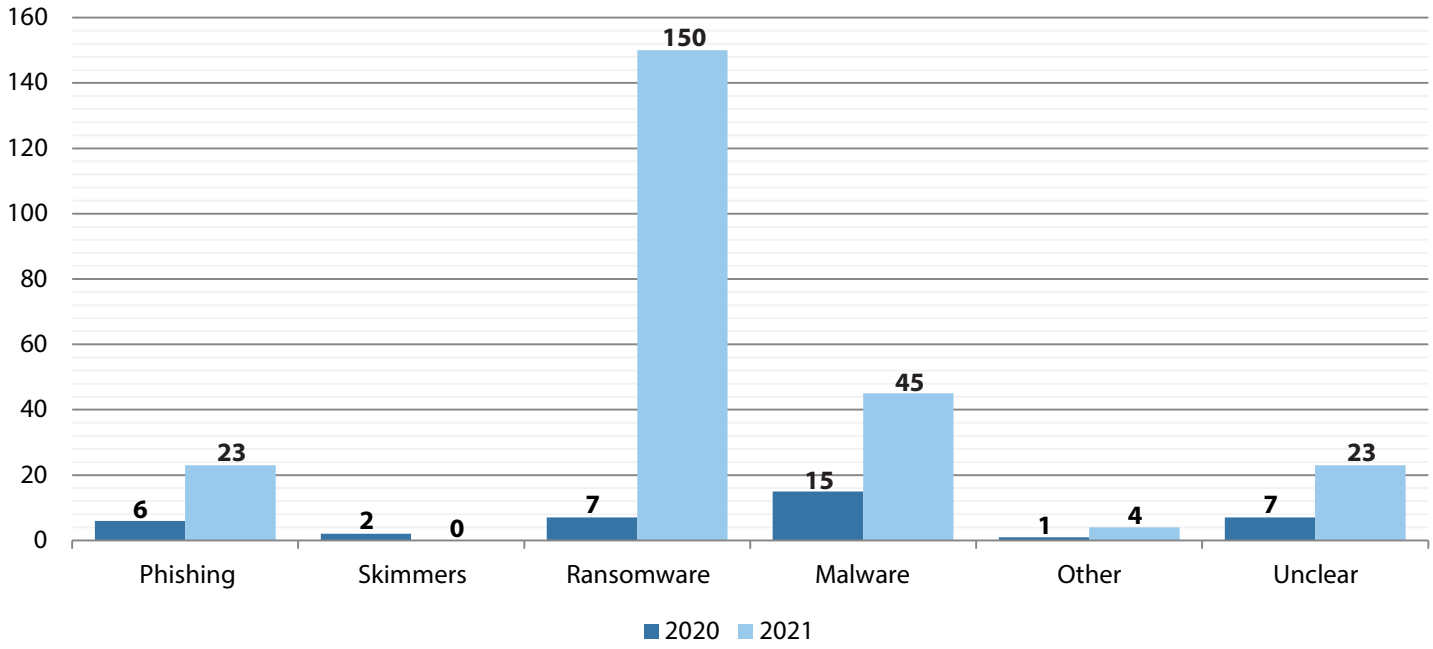
Cyberattacks can occur in a number of ways. Some of the most common methods include:

- **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, that appears authentic. The goal of phishing is to fool the recipient into volunteering 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

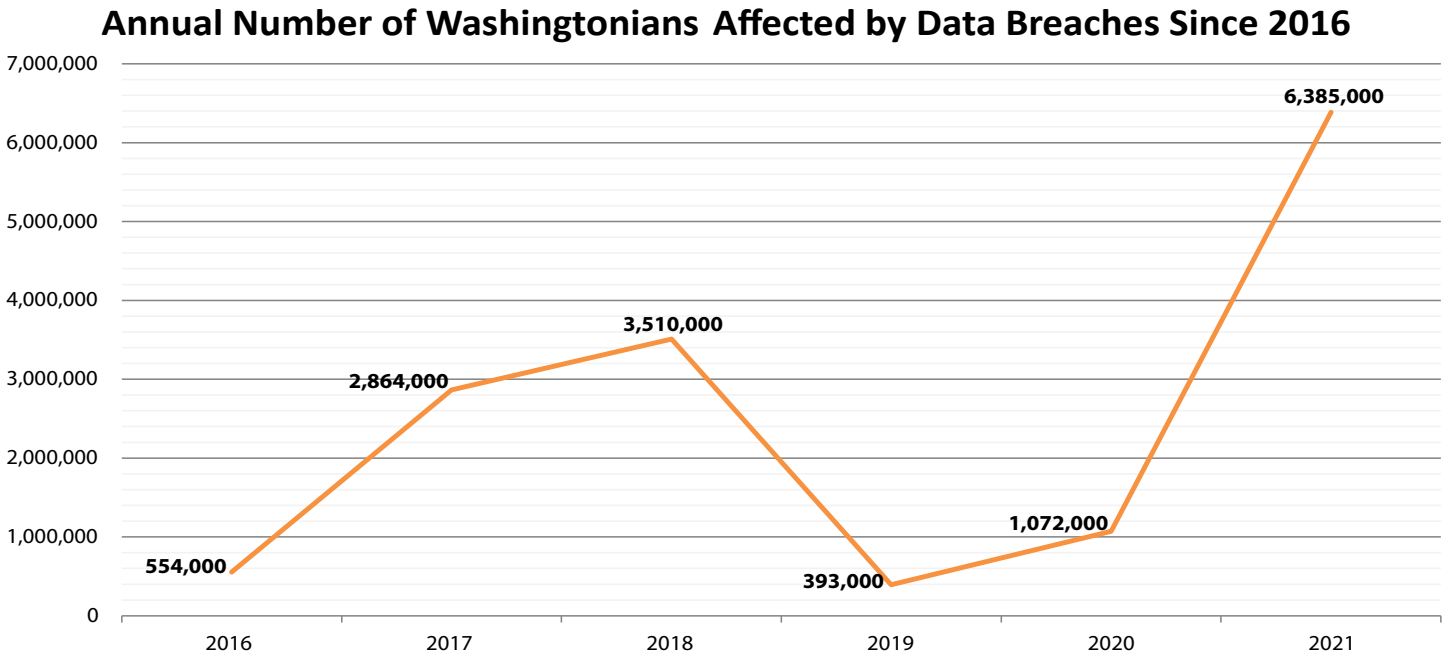
Malicious Cyberattacks by Type in Washington



Our office received notice of 245 breaches caused by cyberattacks in 2021. Of those 245 breaches, 23 of the notices did not provide enough information to discern the specific method of cyberattack. Ransomware was by far the most common cyberattack type in 2021, representing approximately 61% (150) of cyberattacks. This is a significant increase from last year, with only seven such attacks, representing 18% of cyberattacks in 2020.

The larger proportion of ransomware attacks relative to other types is largely a result of the 2020 ransomware attack on the cloud-computing provider Blackbaud. Over one third of the notices submitted to our office in the last year were a result of this single massive ransomware attack. Under Washington law, the owners of the data are required to provide notification of a breach, so the impact of the Blackbaud breach is spread across 100+ notices, rather than a single ransomware attack. However, even if we account for this and treat the Blackbaud incident as a single ransomware breach, the number of remaining ransomware breaches still outnumbers all other types and is greater than the total number of ransomware attacks reported in the last five years combined.

Number of Washingtonians Affected

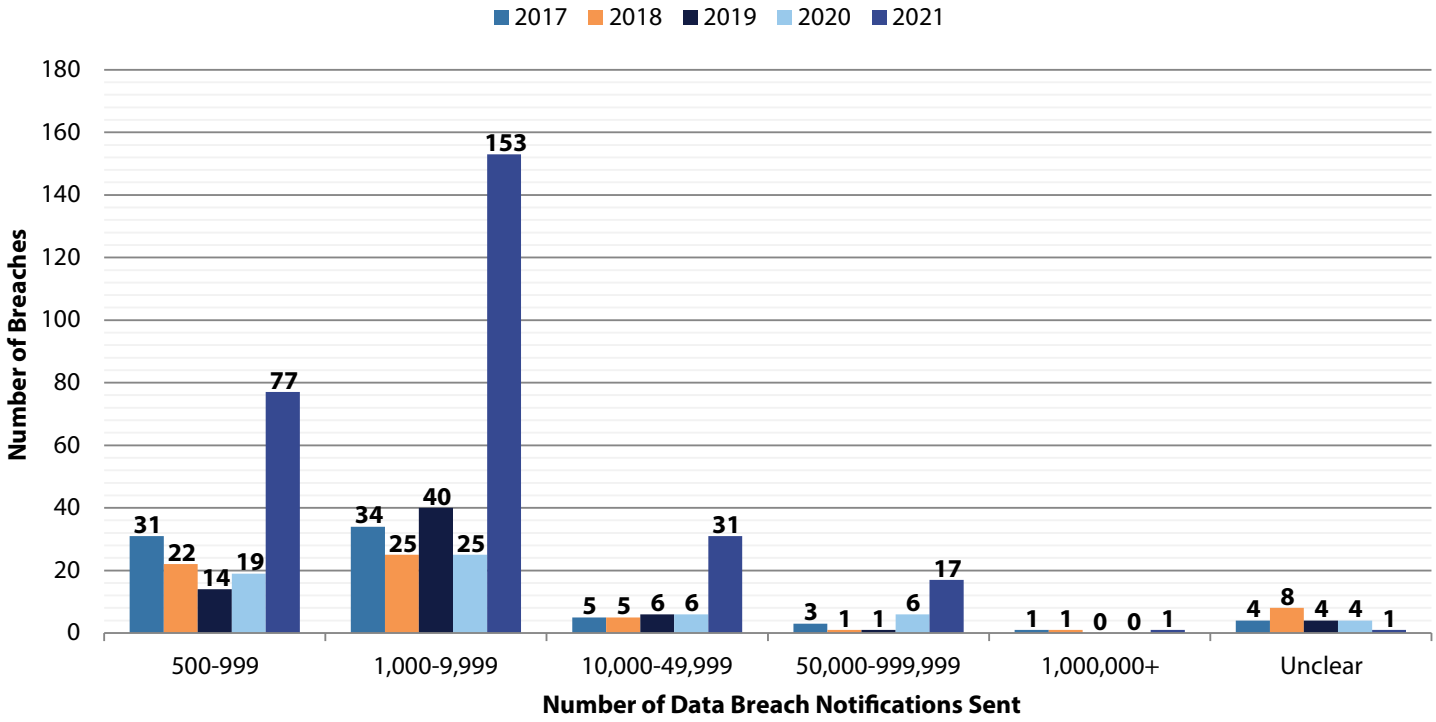


In 2021, business, agencies and other entities reported 280 data breaches affecting more than 500 Washingtonians' personal information. This is up from 2020's 60 reported breaches. The total number of Washingtonians affected increased significantly as well — up 496% from last year, from 1,072,000 in 2020 to approximately 6,385,000 in 2021. This is the highest number of Washingtonians affected by breaches in a single year since our office began tracking this information.

We can attribute this increase to several factors:

- A significant increase in the overall volume of reported breaches, either as a result of the March 2020 update to our state's requirements for notice (which likely expanded the number of breaches covered by the law), an uptick in cybercrime, or both;
- A 200% increase in the number of breaches impacting more than 50,000 Washingtonians compared to 2020; and
- The impact of two breaches in particular, Blackbaud (spread out across 100+ notices), and Accellion as it related to the Washington State Auditor's Office, our first recorded mega breach since 2018.

Washingtonians Affected by Data Breaches

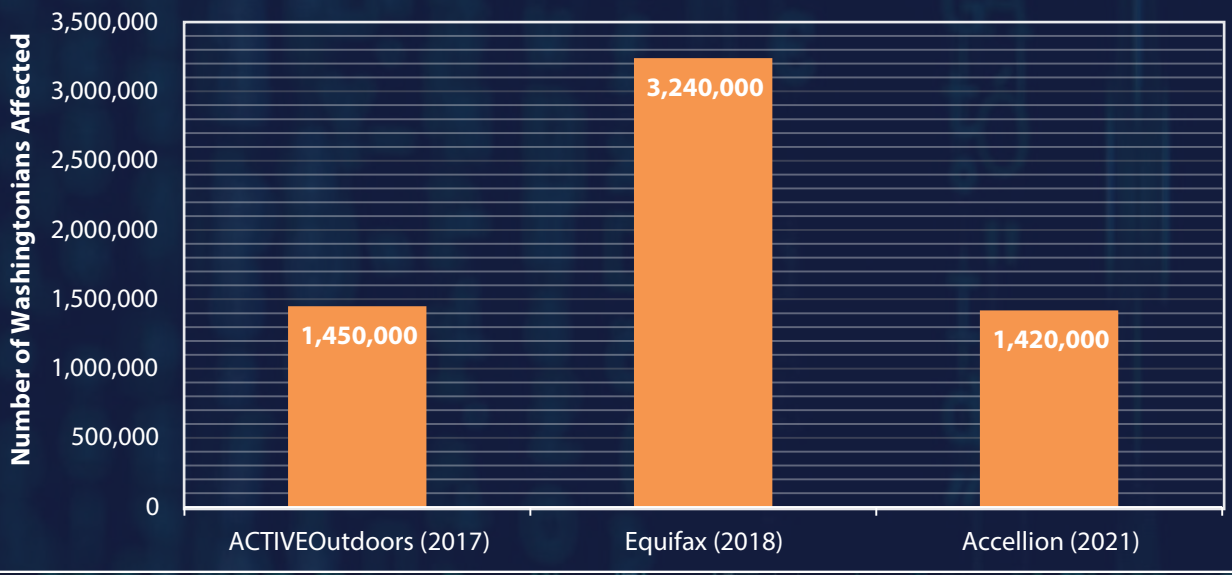


In 2021, the majority of data breaches compromised the personal information of between 1,000 and 9,999 Washington residents. This is the fourth straight year that the majority of breaches affected at least 1,000 Washingtonians. 2021 sets a new high for number of breaches affecting between 1,000–9,999 Washington residents since our office started tracking this data, at 153 breaches, topping the previous high in 2019 of 40.

What are "Mega Breaches"?

For the purposes of this report, a mega breach is any breach that affects the personal information of one million or more Washington residents. When they occur, these breaches have a tremendous impact on the total number of Washingtonians impacted by data breaches each year, generally affecting more people in a single breach than all other breaches from a single year combined.

Mega Breaches Affecting Washingtonians Since 2016



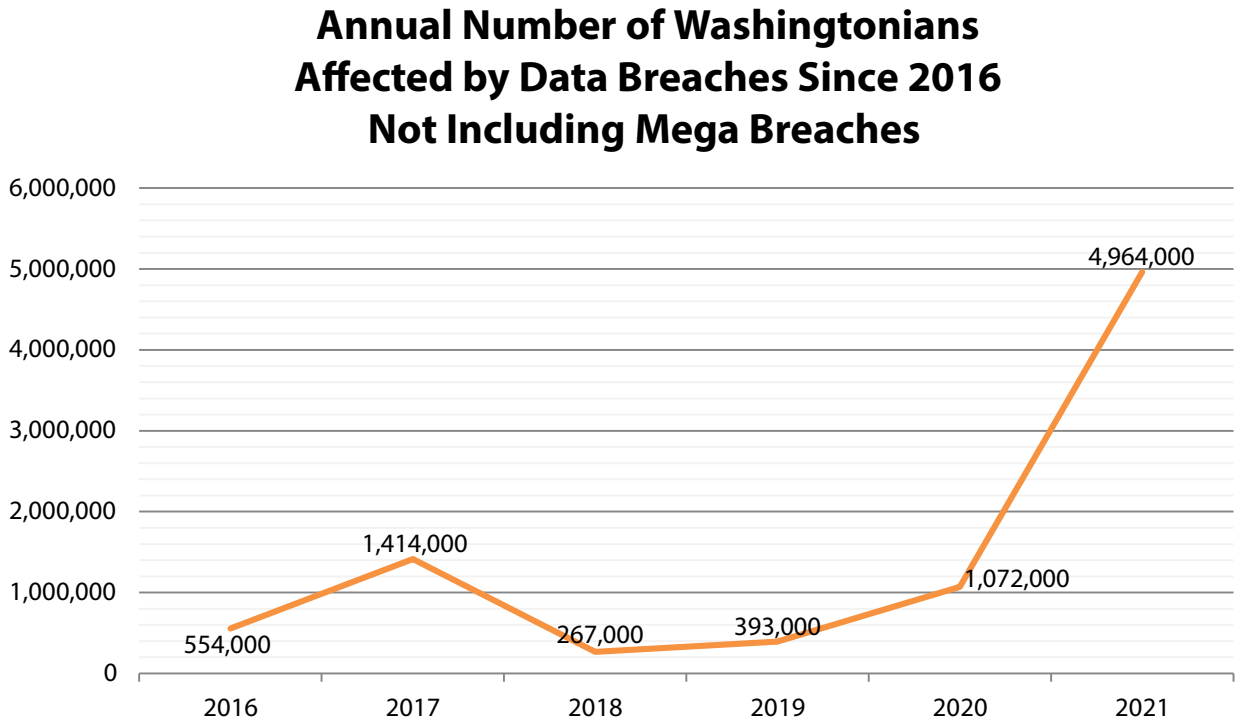
Since our office began issuing this report in 2016, the AGO received notices of three confirmed mega breaches — the ACTIVEOutdoors breach in 2017, the Equifax breach in 2018, and this year's breach of Accellion as it related to the Washington State Auditor's Office.

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 2021 "Cost of a Data Breach Report," breaches compromising 1 to 10 million records cost breached entities an average of $52 million per breach, while breaches affecting more than 50 million records cost an average of $401 million per breach.[1]

While not technically a mega breach by this report's definition, due to being spread out across over one hundred separate notices, the influence of the Blackbaud breach on this year's data is nevertheless worth noting. This single ransomware incident is responsible for more than 3 million of the impacted Washingtonians in this year's report, and includes breaches of more than 60 non-profit and charitable organizations, and over 30 academic institutions. The vast majority of notifying data owners reported breaches of names and dates of birth, though several breaches also exposed Social Security numbers, financial information, and other sensitive forms of personal information.

In addition to the Blackbaud breach, the 2021 mega breach of Accellion that affected the Washington State Auditor's Office (SAO) significantly influenced this year's data. This is yet another example, similar to Blackbaud, where the breach was not of the notifying entity's systems, but of a third-party vendor that was managing their data. In this case, the impacted vendor was Accellion, a company that specializes in file sharing technology. The cyberattack on Accellion compromised files in the possession of SAO. These files contained the personal information of approximately 1.3 million Washingtonians, including residents' names, Social Security numbers, dates of birth, bank account and routing numbers, addresses, and email.

Due to their massive size, mega breaches like Accellion can obscure trend data for the more common small to midsize 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 from 2018 to 2019, and more than doubled in 2020. In 2021, the total number of Washingtonians affected grew by an additional 363%, resulting in entities sending nearly 5 million notices to Washington residents. The Blackbaud breach drives this huge spike — although even if we remove these notices from the data, the number of Washingtonians impacted is still around 1.5 million, a 40% increase from 2020.

Types of Personal Information Compromised

Washington law requires notification to the Attorney General's Office when a data breach includes personal information (PI). Washington defines PI as:[2]

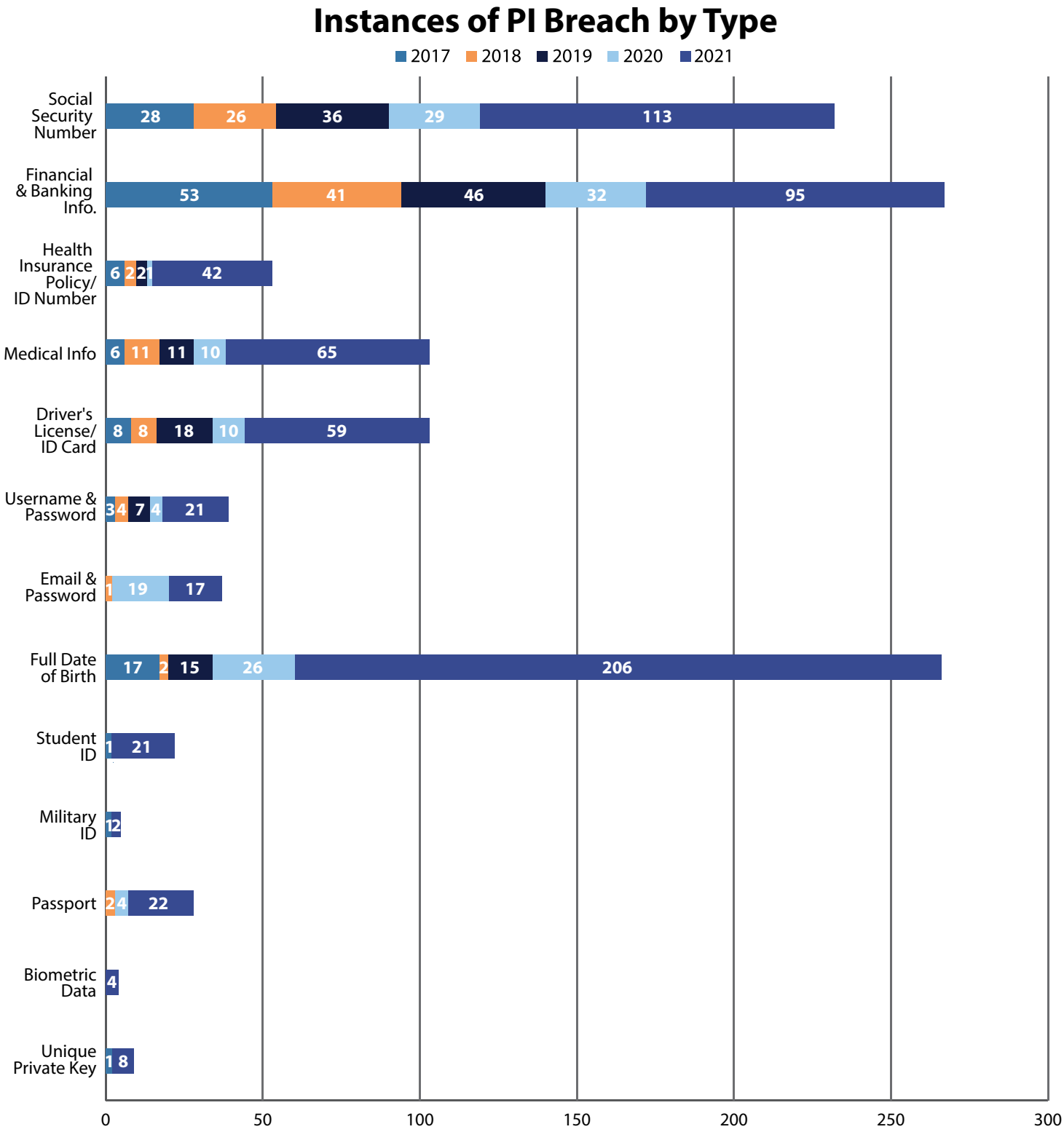
An individual's first name or first initial and last name in combination with any of the following:

- **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.

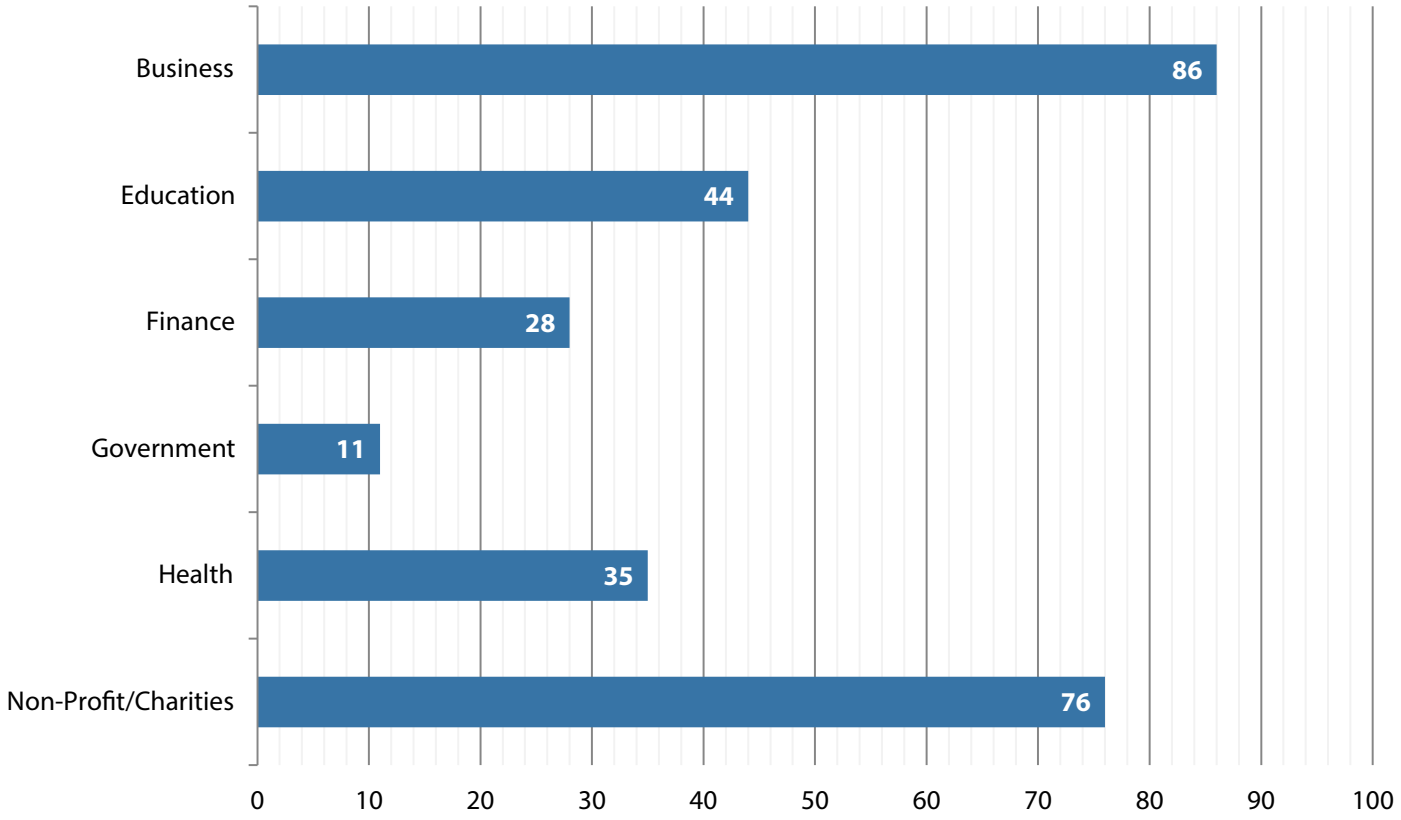


In 2021, 206 breaches, representing nearly three quarters (74%) of all breaches reported this year, resulted in the compromise of a Washingtonian's name and date of birth. This is the first time since 2016 that financial information did not lead this category.

However, consistent with previous years, Social Security numbers were the second most commonly compromised PI component, with reported impacts in 40% (113) of breaches. Of the new elements added to the definition of personal information in 2020 — aside from date of birth — username in combination with a password and passport numbers saw significant increases compared to last year's report; growing by 425% (21) and 450% (22), respectively. This was also the first time entities reported the exposure of student identification numbers since their addition to the notification law, with exposure occurring in 8% (21) of breaches.

Industries Reporting Breaches

Number of Breaches in 2021 by Industry



The Attorney General's Office also tracks breaches by industry. Consistent with earlier reports, our office uses the following industry categories:

Business **Education** **Financial Services** **Government** **Health Care**

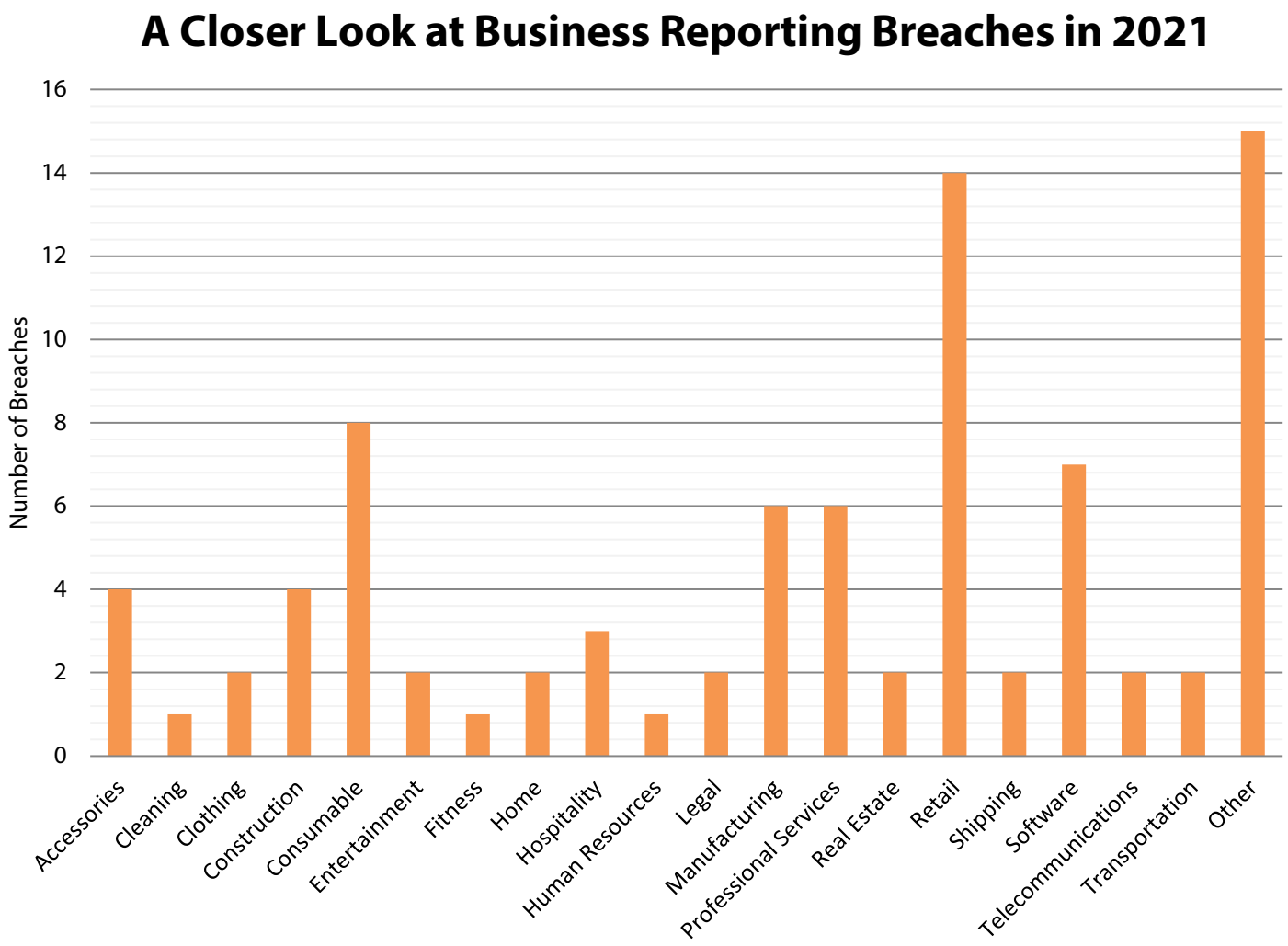
However, for this year's report the AGO is adding a sixth category:

Non-Profit (NPO) & Charitable Organizations

In previous reports, our office treated NPOs and charities as a sub-category of businesses. However, due to the unique nature of these organizations, as well as their central role in the 2020 Blackbaud breach, we established a separate category for analysis this year.

With this change, the business category now includes 23 sub-categories, including retail, manufacturing, transportation, construction, hospitality, and software.[3]

For a fourth straight year, organizations categorized as businesses reported more breaches than any other industry, accounting for 31% of all breaches in 2021, of which cyberattacks comprised 79%. Of these, 44% were cyberattacks perpetrated using malware, such as having malicious code installed onto servers or websites. An additional 32% were caused by a ransomware attack.



Aside from "Other," the retail (16.2%) and consumable (9.3%) sub-categories were the most common types of businesses to be breached, together representing just over a quarter of all breaches reported by businesses in 2021.

Non-profit and charitable organizations followed just behind businesses, accounting for 27% of breaches in 2021. Despite being second in total breaches, the NPO category had the largest total number of affected Washingtonians, 2.8 million, driven by the Blackbaud breach. Breaches of NPOs in 2021 affected on average 37,132 Washingtonians per breach, and accounted for 44% of all notices sent to Washingtonians impacted by data breaches in 2021. This is up significantly from 2020, when breaches affecting NPOs accounted for just 2% of impacted Washingtonians.

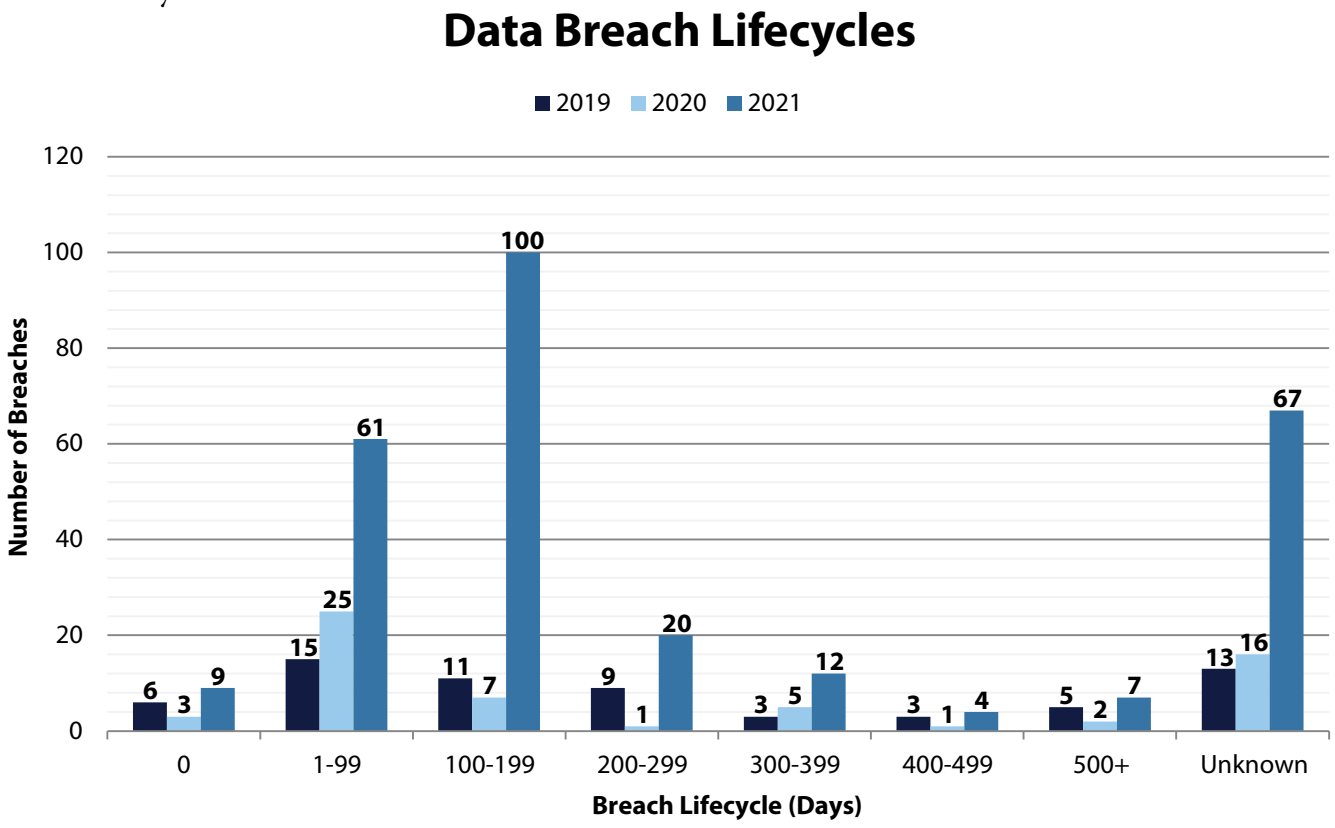
Time to Resolve Data Breaches

What is a Data Breach "Lifecycle"?

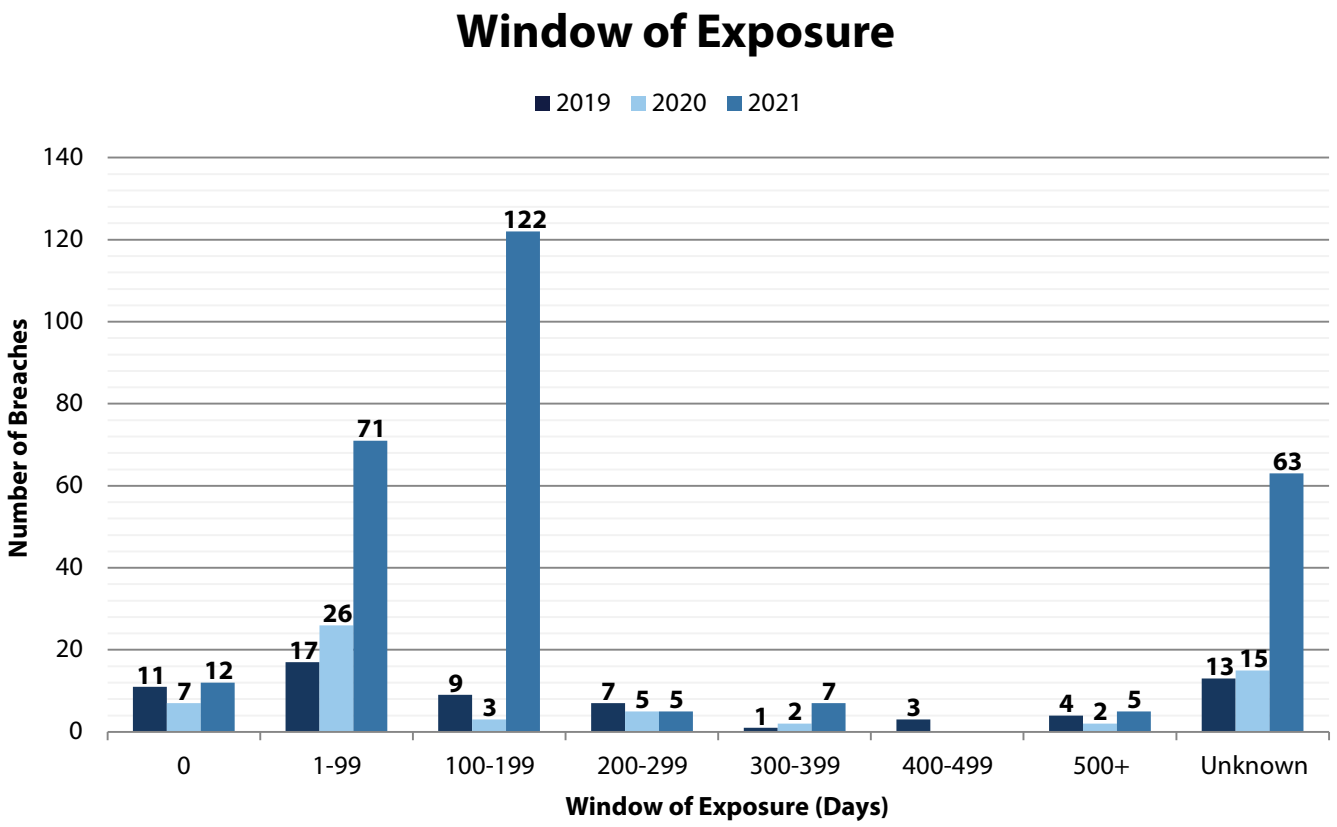
Resolution of a breach involves two steps:

1. Identification of the breach's occurrence; and
2. Subsequent containment of the breach.

In this report, our office 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 total time to resolve a data breach is the sum of these two measurements. This is the "lifecycle" of a breach.



This differs from the period of time in which a breach is active, also known as the "window of exposure." Sometimes the theft of information concludes before its discovery by the breached entity. This was the case in 145 (52%) of the breaches reported to the Attorney General's Office in 2021. In scenarios like these, the window of exposure can be significantly shorter than the lifecycle of a breach, as it can take time for an organization to understand what has occurred and secure its systems.



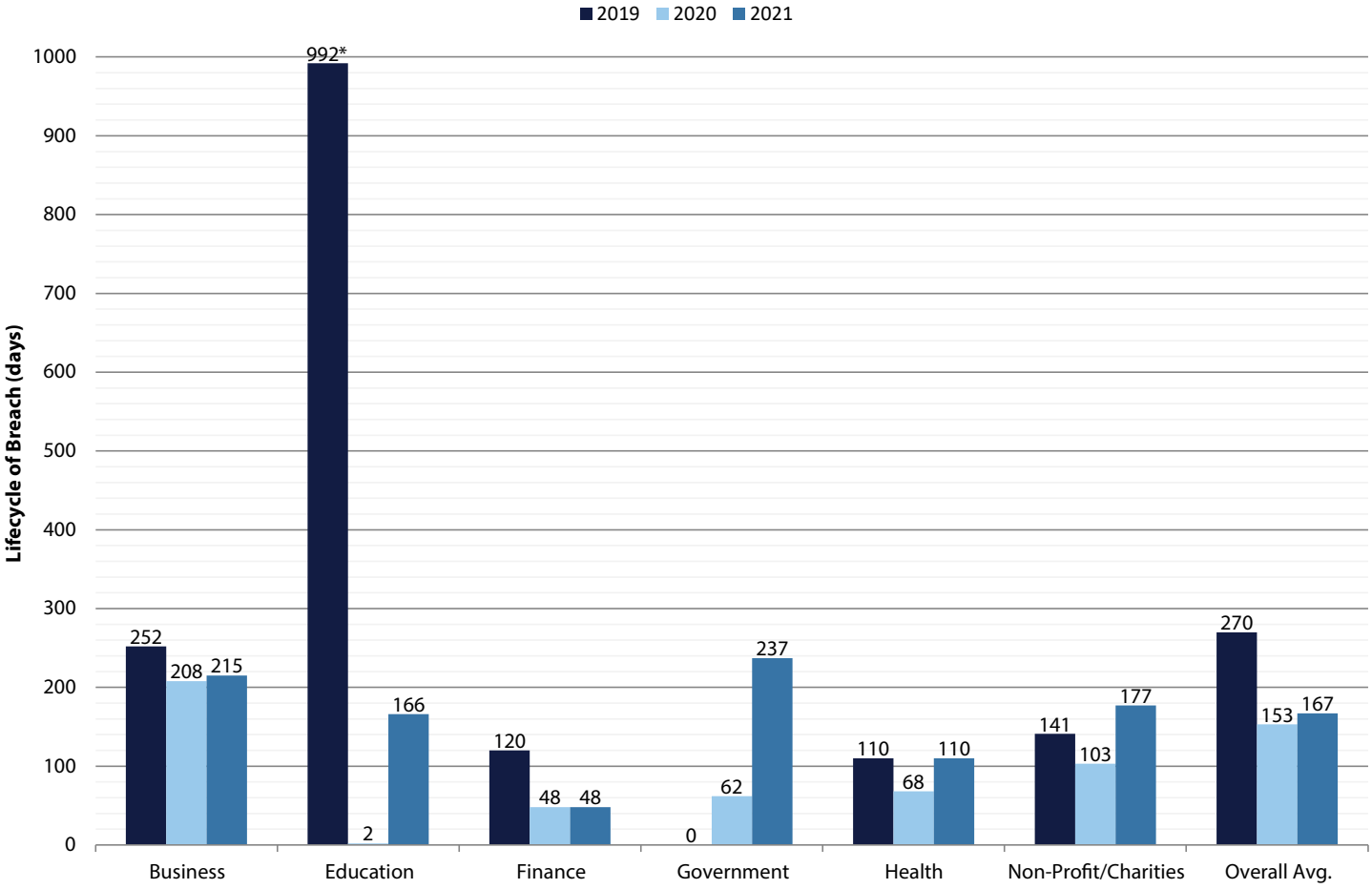
An example of this includes a breach reported to our office by Grays Harbor Community Hospital (GHCH) on January 29, 2021. In this case, GHCH reported that one of their third party vendors that provided GHCH with mail processing services informed the hospital of a ransomware incident affecting the personal information of some of their patients. The ransomware attack occurred between May 6, 2019 and May 15, 2019. This represents a window of exposure of approximately 9 days.

However, GHCH did not become aware of this incident until their vendor notified them on November 29, 2020 — 573 days after the breach began. As a result, the lifecycle of this breach (573 days) was longer than the window of exposure (9 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 majority of data breaches in 2021 had both a window of exposure and lifecycle between 100 to 199 days. On average, breaches with a lifecycle of 100 to 199 days affected 34,062 Washingtonians per breach in 2021.

There were also a significant number of breaches in 2021 where the window of exposure or lifecycle could not be determined from the notification provided to our office, categorized as "Unknown." In 2021, there were 67 cases where the lifecycle of the breach could not be determined. On average, these incidents affected 29,661 Washingtonians.

Average Lifecycle of Breaches Affecting Washingtonians by Industry



**Note: The 2019 average for Education is heavily influenced by the Yale University breach, reported to our office in July of 2018, which was not discovered for 3,728 days. Without this data point, the average lifecycle of a breach for Education in 2019 was 80 days.*

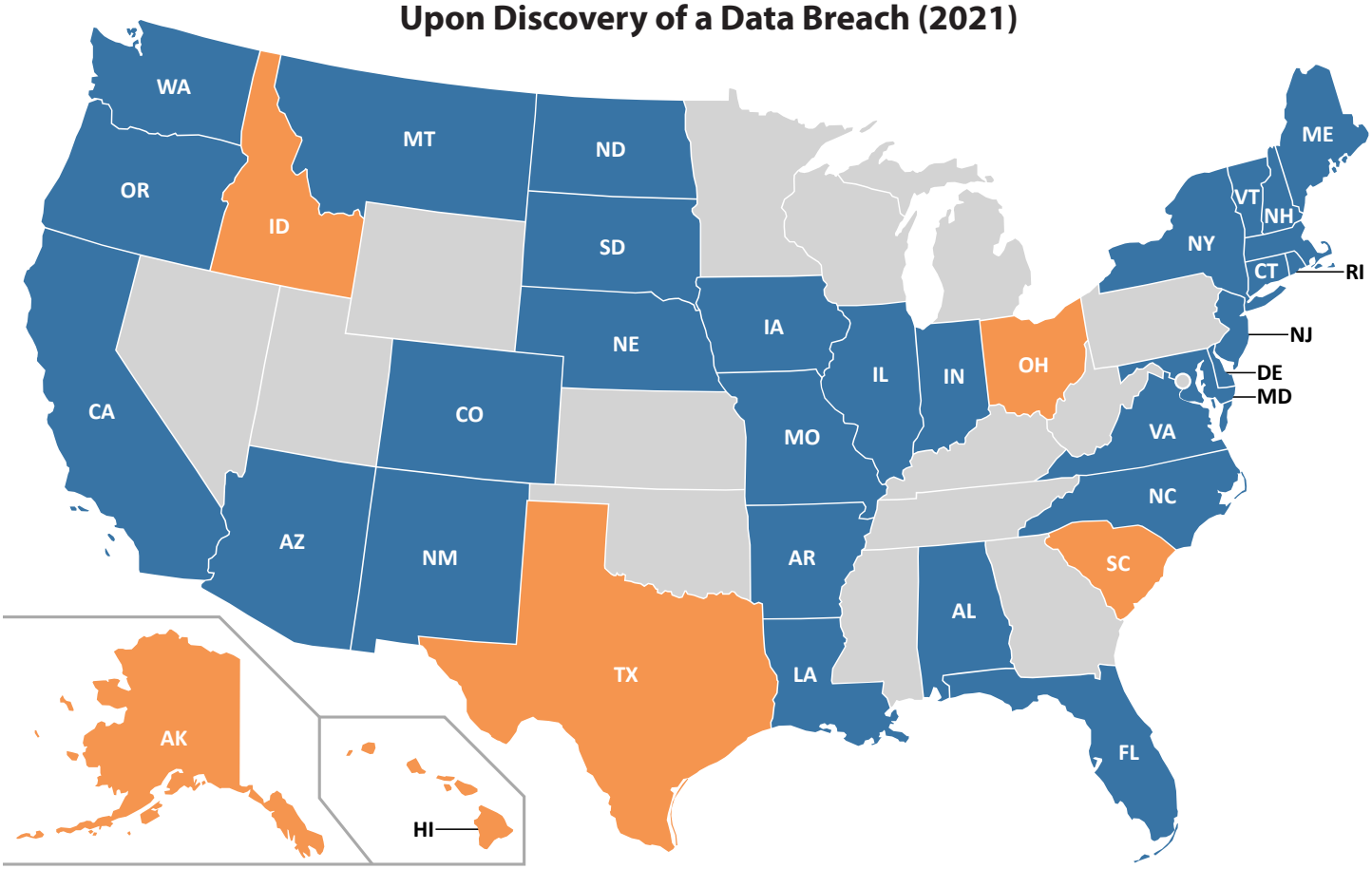
The Average Lifecycle of Breaches by Industry

The average lifecycle of a breach increased for all industries in 2021 except finance, which remained at an average of 48 days. According to the Ponemon Report, in 2021 organizations that resolved data breaches in fewer than 200 days saved, on average, $1.26 million per breach compared to their counterparts who took more than 200 days.[4] Notably, the Ponemon Report also states that the global average lifecycle of a breach across all industries in 2021 was 287 days. On average breaches had a lifecycle of 167 days, a 9% increase from 2020 when the average was 153 days.

The fact that the average lifecycle of a breach in 2021 remains above 100 days is indicative of the continued difficulty of detecting breaches as cybercriminals increasingly rely on more complex and covert methods of breaching security systems, including ransomware.

State Data Breach Notification Laws: How does Washington's Law compare to other states?

States Requiring Notification of State Attorney General Upon Discovery of a Data Breach (2021)



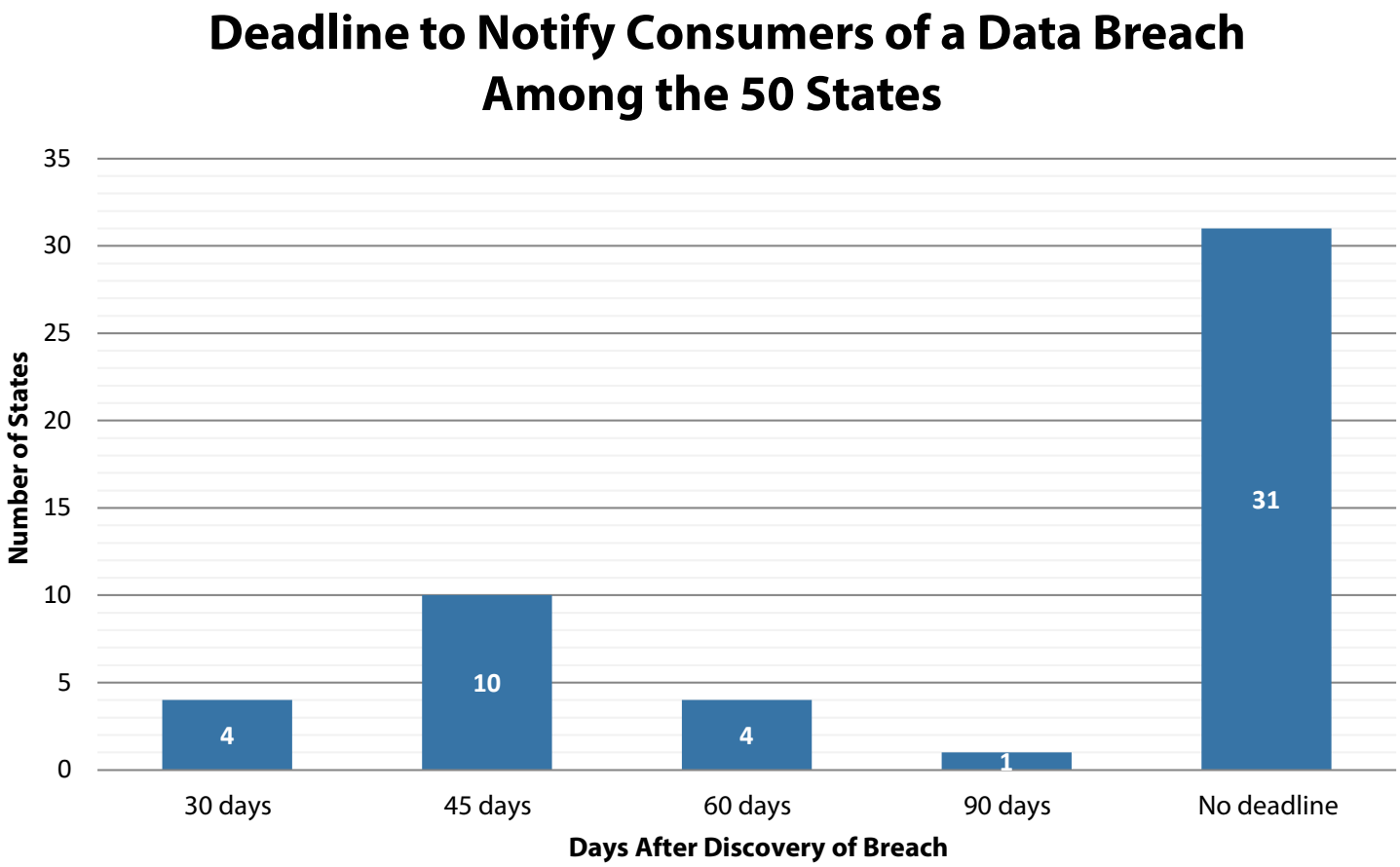
*States in orange only require notification to the Attorney General under special circumstances (e.g. Idaho only requires notice from public agencies), and/or require notification to a state agency that is not the Attorney General (e.g. Hawaii requires notice to the Office of Consumer Protection).
Data for this map was derived from: Perkins Coie. (2020, June). "Security Breach Notification Chart." Accessed August 2021, from https://www.perkins-coie.com/en/news-insights/security-breach-notification-chart.html

Washington Compared to Other States

All 50 states have laws requiring private or governmental entities to notify individuals when a data breach occurs.[5]

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 has been breached together with the encrypted information.[6]

In 36 states, including Washington, entities experiencing a breach must notify the Attorney General or another state agency.[7] 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.[8] In Iowa, a breached entity is required to provide notice to the Director of the Consumer Protection Division at the Attorney General's Office if it affects more than 500 Iowa residents, and must do so within 5 days of providing notice to consumers.[9] Unlike Washington, however, neither state has an explicit deadline to notify consumers for breaches affecting private entities.



In fact, only 19 states, including Washington, have a specific deadline for reporting breaches to consumers.[10] As of September 2020 Washington, Colorado, Florida and Maine have a 30 day deadline to notify consumers, the shortest deadline in the country**.**

Most states with a deadline, including Washington (RCW 19.255.010 (16)), trigger the timeline upon discovery of a breach of personal information and require that notification "be given in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."

How Other States Define Personal Information

All 50 states have 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 in the updated 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 ten other states.

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, Florida, Maryland, Vermont, Virginia, ***Washington***, Wyoming
Passport ID Number	Alabama, Arizona, California, Colorado, Delaware, Florida, Louisiana, Maryland, North Carolina, Oregon, Vermont, Virginia, ***Washington***
Health insurance policy number	Alabama, Arizona, California, Colorado, Delaware, Florida, Illinois, Maryland, Missouri, Nevada, North Dakota, Oregon, Rhode Island, Virginia, ***Washington***, Wyoming
Medical/Health information	Alabama, Arizona, Arkansas, California, Colorado, 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, 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, Delaware, Florida, Illinois, Maryland, Nebraska, Nevada, New Jersey, New York, Oregon, South Dakota, ***Washington***, Wyoming
Email address and password	Alabama, Arizona, California, Colorado, Delaware, Florida, Illinois, Maryland, Nebraska, Nevada, New Jersey, New York, Rhode Island, South Dakota, ***Washington***, Wyoming
Individual Taxpayer ID number	Alabama, Arizona, California, 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, need not be in combination with an individual's name to trigger the notification statute.[11]

Massachusetts' law, conversely, requires names to be part of the breach of financial information to trigger notice, but not passwords or security codes.[12] 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.[13]

At the time of publication, Washington's law stands out by defining more elements of personal information (15) than any other state. 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 (page 22).

Conclusion and Recommendations

Data breaches continue to be a significant concern for Washingtonians in 2021 and beyond. With the impacts of the Blackbaud and Accellion breaches, 2021 is the most significant year for data breaches since our office began tracking this information in 2016. In total, our office received 280 data breach notices affecting more than 500 Washingtonian's personal information, which is *more than the past four years combined*. Entities sent more than 6 million data breach notices to Washingtonians in 2021, a 496% increase from 2020, and more than the combined total number of notices sent to Washingtonians from 2018 to 2020.

The growing number of Washingtonians affected by breaches this year further highlights the importance of the data breach notification legislation passed in the 2019 legislative session. Thanks to the improvements made to the law, entities that experienced breaches were required to provide earlier and more detailed notices to consumers in 2021.

However, even with these important updates, opportunities remain for policymakers to continue strengthening our state's data breach notification law. Potential improvements include:

1. **Amending the definition of "personal information" in RCW 19.255.005 to include full name in combination with a redacted SSN that still exposes the last four digits of the number;**

SB 6187 — which Governor Inslee signed into law on March 18, 2020, and went into effect on June 11, 2020 — modified the definition of personal information for breaches that occur at local and state agencies. Specifically, the bill modified the definition of personal information in RCW 42.56.590 to include the last four digits of a Social Security number in combination with a consumer's name as a standalone element that will trigger the requirement for consumer notice. This change should extend to RCW 19.255.005 as well, to bring both laws into alignment, and provide consumers with the most robust protections possible, regardless of the type of entity that was breached.

2. **Amending the definition of "personal information" in RCW 19.255.005 and RCW 42.56.590 to include Individual Tax Identification numbers (ITINs).**

The IRS 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, 10 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.[14] These Washingtonians deserve the same protection that those with Social Security numbers have.

Appendix

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 Washington Attorney General'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 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 Washington Attorney General's Office 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.

Best Practices for Avoiding and Mitigating Ransomware Attacks

Due to the unique nature of ransomware attacks, organizations and individuals should utilize best practices to limit their exposure. Per the FBI's guidance (https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware), entities should:

- Keep operating systems, software, and applications current and up to date;
- Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans;
- Back up data regularly and double-check that those backups were completed; and
- Secure those backups, and make sure they are not connected to the computers and networks they are backing up.

Additionally, the FBI does not support the practice of paying a ransom in response to a ransomware attack, noting that paying a ransom does not guarantee the return of any data, and also incentivizes perpetrators to target more victims.

If you are a victim of ransomware:

- Contact your local FBI field office to request assistance, or submit a tip online; and
- File a report with the FBI's Internet Crime Complaint Center (IC3).

Washington's Data Breach and Data Security Laws

Requirements to Provide Notification

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 Attorney General's Office must also receive notice when a data breach requires notification of more than 500 Washington residents. The notice to consumers and the Attorney General 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 Attorney General 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 Attorney General's Office if any of the required information is unknown at the time the notice is due.

A list of all data breach notices that our office has received 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, which Governor Inslee signed into law on March 18, 2020, and went into effect on June 11, 2020, 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 Attorney General's Office 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 (RCW 19.255.010(10)).

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 this year's 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 common if the breached organization does not have a dedicated cybersecurity team on staff and has to 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 based on what we know as of August 20, 2021.

Over the course of this summer, 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. It is our hope that this form will lead to more accurate and complete information regarding data breaches affecting Washingtonians, as well as a more efficient notification process for everyone involved. This web form is available at https://fortress.wa.gov/atg/formhandler/ago/databreachnotificationform.aspx.

Additionally, building these new resources provided our office the opportunity to audit and update our existing data. As such, you may notice that our office has revised several statistics reported in past years with more complete and accurate information. Of particular note, the total number of Washingtonians in 2020 increased from the 651,000 figure we reported last October, to an updated total of 1,072,000. This was due to the addition of a breach at Morgan Stanley that affected more than 400,000 Washingtonians, which was not available until February of 2021.

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.

As such, 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 be accounted for 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
- Sahar Fathi, Policy Team
- Ellen Austin Hall, Policy Team
- Anthony Pickett, Administration
- Mike Webb, Chief of Staff
- Donnelle Brooke, Consumer Protection Division
- Joe Kanada, Consumer Protection Division
- Andrea Alegrett, Consumer Protection Division
- Melisa Dolby, ISD
- Kaya Imamura, ISD
- Maria Andreas Nazy, ISD
- Brionna Aho, Public Affairs
- Beth Carlson, Public Affairs
- Ian Couch, Public Affairs
- Dan Jackson, Public Affairs
- Stacia Hollar, Government Compliance and Enforcement Division
- Matthew Kernutt, Government Compliance and Enforcement Division

Notes and Citations

1. Ponemon Institute. (2021, July). "2021 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. (2021, July). "2021 Cost of a Data Breach Report."
5. Perkins Coie. (2020, June). "Security Breach Notification Chart." Accessed August 2021, from https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.
6. Ibid.
7. Ibid.
8. Idaho Code § 28-51-104 (2006); as amended (2010).
9. Iowa Code § 715C.1-2 (2008); as amended (2018).
10. Perkins Coie. (2020, June). "Security Breach Notification Chart." Accessed August 2021, from https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.
11. Colo. Rev. Stat. Ann. § 6-1-716 (2006); as amended (2018).
12. Mass. Gen. Law Ann. Ch. 93H, §§ 1 (2007).
13. Ind. Code Ann. §§ 24-4.9 et seq. (2006); as amended (2009).
14. 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.