WASHINGTON STATE ATTORNEY GENERAL'S OFFICE

2020

DATA BREACH REPORT

TABLE OF CONTENTS

LETTER FROM THE ATTORNEY GENERAL

October 2020

Dear Washingtonians,

Data breaches are a significant ongoing threat to Washington residents, businesses, and agencies. In 2020, the total number of breaches reported to our office decreased by 15%, and yet the total number of Washingtonians impacted by breaches rose by 67%, with nearly 65% resulting from a malicious cyberattack.

During the past year, a diverse set of organizations experienced data breaches, including retailers, financial services, nonprofits, and healthcare providers. Breaches befell these organizations in a variety of ways. In particular, an increasing number of organizations are dealing with attacks known as "ransomware," in which a cybercriminal uses a unique type of malware that holds data hostage in hopes of receiving a ransom payment from the data holders.

In response to these alarming trends, which have been detailed in each of our annual Data Breach Reports over the last five years, I requested legislation during the 2019 legislative session to strengthen our state's data breach laws. This legislation, which unanimously passed both the House and Senate, expands our state's definition of personal information to include more types of consumer data and reduces the deadline to notify consumers from 45 to 30 days. These changes went into effect on March 1, 2020.

As a result of this legislation, Washington now has one of the most robust Data Breach Notification laws in the country. This, in combination with being one of only four states with the shortest deadline for consumer notice (30 days) and one of the only states who continue to track and publish figures on data breach incidents and laws, has established Washington as a clear leader on the issue of data breaches nationally.

This report presents a summary of the data breach notices my office received over the past year. Tips and resources for consumers and businesses are included at the end of the report.

I hope you find this information helpful.

Sincerely,

Bob Ferguson
Washington State Attorney General

Executive Summary

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 within 30 days of discovering the breach, as well as to notify the Attorney General's Office if more than 500 Washingtonians are impacted as a result of the breach.

In 2019, Attorney General Ferguson proposed, and the Legislature passed, a bill strengthening Washington's data breach notification law. This legislation, sponsored by Rep. Shelley Kloba and Sen. Joe Nguyen, significantly expanded the state's 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, and firmly cemented Washington State as a national leader on data breach policy. This year's Data Breach Report is the first to be published by our office since the amended law went into effect.

This 2020 report is based on data breach notifications received by the Attorney General's Office between July 24, 2019 and July 23, 2020 that affected more than 500 Washingtonians' personal information. Additional information on our data gathering process can be found in the "Data Analysis Methodology" section on page 6. This year's data reveals:

- 33 cyberattacks were reported to our office in 2020, representating a decrease from 2019 when 43 cyberattacks were reported. Approximately 65% of all breaches reported in 2020 were a result of cyberattacks, also down from 2019 when about 72% of breaches were caused by cyberattack. Notably, instances of ransomware tripled compared to 2019.

- Fewer breaches were reported to our office in 2020, decreasing from 60 reported breaches last year to 51 this year. However, the total number of Washingtonians affected by data breaches increased by 67%, from 390,000 in 2019 to 651,000 in 2020.

- For a third straight year, the majority of data breaches reported to our office impacted the personal information of between 1,000 and 9,999 Washington residents.

- For a second year in a row, no mega breaches impacting the personal information of 1 million or more Washingtonians were reported to our office.

- For a fifth straight year, financial information was the most commonly compromised type of personal information, impacted in 57% of reported breaches, followed by Social Security numbers, which were compromised in 47% of reported breaches. Of the new elements added to the definition of personal information in 2020, date of birth and email in combination with a password were the most prevalent, represented in 39% and 35% of breaches, respectively. A full list of the elements included in the definition of personal information can be found in the "Washington's Data Breach & Data Security Laws" section on page 21.

- For a third straight year, the majority of breaches reported in 2020 came from organizations categorized as businesses, which accounted for nearly 63% of all breaches. Of these breaches, approximately 60% were the result of malicious cyberattacks, of which about 63% were perpetrated through the use of malware, such as having malicious code installed onto servers or websites.

- The average lifecycle of a breach decreased for all but one industry in 2020. On average, breaches reported to the Attorney General's Office had a lifecycle of 148 days, a 47% decrease from the 2019 average of 277 days. This data suggests that 2019's lifecycle data may have been an outlier.

Recommendations

While the update to the Data Breach Notification law in March is a major step forward for informing consumers about data breaches when they happen, opportunities remain for policymakers to continue strengthening our state's laws protecting the personal information of Washingtonians. The Attorney General's Office recommends that policymakers:

1. **Expand the definition of "personal information" in RCW 42.56.590 to include the last four digits of a Social Security number. In the 2020 legislative session, SB 6187 was signed into law expanding the definition of personal information to include this data when it is involved in the breach of local or state agency. This expansion to the definition should be extended to private entities and federal agencies as well, via an amendment to the definition of personal information in RCW 19.255.005.**

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

3. **Require persons or businesses that store personal information to maintain a risk-based information security program, and to ensure that personal information is not retained for a period longer than is reasonably required.**

The Insidious and Unpredictable Harms of Data Breaches

Data breaches matter because there is a risk of harm whenever an unknown entity gains access to consumers' personal information. Despite this, many consumers continue to underestimate the scope of this threat.[1]

There are a number of reasons this may be the case, including:

- Consumers becoming desensitized to data breaches due to the sheer volume of incidents that have occurred over the last decade;
- The impacts of most data breaches are not usually felt right away, and sometimes not for a significant amount of time, potentially giving consumers a false sense that breaches aren't much of a threat; or
- A change in priorities motivated by other more immediate or obvious threats (e.g. COVID-19, wildfires, etc.).

As a result, many consumers may be under the impression that most breaches are not a significant threat, or that they are all relatively the same.

These same consumers might imagine a worst case data breach looking something like this:

1. A business is hacked by a cybercriminal;
2. The cybercriminal is able to gain access to a consumer's personal information, like full name, credit card number, card expiration date, and CVV;
3. The cybercriminal then makes purchases with the consumer's stolen card information;
4. The business discovers the breach, and notifies the consumer (or vice versa);
5. The consumer is urged to cancel their debit/credit cards, change their passwords, reset their account information, and take other protective measures;
6. The business repairs the gap in their cyber security, and the breach is resolved.

Unfortunately, while some breaches play out this way, many are not so cut and dry.

In fact, rather than put a consumer's stolen data to use right away, many cybercriminals instead will list their personal information for sale on a digital black market.[2] This isn't just credit card information, but everything from medical records, personal files (like photographs), purchasing habits, job title, Social Security numbers, wage information, tax numbers, and more. From here, a consumer's information could be sold to anyone (or any organization) for any number of purposes: targeted advertising, fraud, and even trolling/harassment, as we saw with the rise of "Zoombombing" earlier this year.[3]

While efforts have been made in recent years to generate tools for consumers to find their information on the dark web, it is impossible to scan every potential website on the dark web for a consumer's data.[4] Even in the event that a consumer's data is found, there is generally very little, if anything, a consumer can do to reclaim their information once it is stolen.

And since the information stolen in a data breach is typically digital, practically infinite copies of the data may exist in these markets. Even if a consumer manages to get their information removed from one place, it is highly likely that it would continue to be available for sale on various other sites. This trend is only exacerbated by the ongoing expansion of stolen data on these digital black markets, which continue to grow each year as more and more breaches occur, including "mega breaches" like Yahoo's August 2013 breach, which impacted 3 billion accounts worldwide, or Equifax's 2017 breach, which impacted nearly 150 million Americans.

This leads us to a difficult truth: statistically speaking, it is highly likely that a significant amount of Washingtonians' personal information, including Social Security numbers, has already been stolen and is readily available on the digital black market.[5] The more information that is stolen, unaccounted for, and made available on these markets, the easier it is for cybercriminals to gain access to and combine different elements of a consumers' personal information to commit acts of fraud or additional data breaches in the future.[6]

This, according to Washington's Employment Security Department (ESD) Commissioner, Suzi LeVine, contributed directly to the widespread unemployment fraud that occurred in May of 2020, resulting in the theft of hundreds of millions of dollars. According to a statement from Commissioner LeVine on May 18, 2020, "This is happening because bad actors have acquired people's personal information through other data breaches outside of the agency. Criminals then use this information to fraudulently apply for unemployment benefits in someone else's name."[7]

This added undue stress and made it more difficult for thousands of Washingtonians whose identities were stolen outside ESD's system to collect unemployment benefits when they needed them most, in the midst of a global pandemic.

This is a sobering conclusion that only further reinforces why it is so critical that we prevent as many data breaches as we can moving forward, and ensure that consumers receive timely notice when breaches do occur.

Data Analysis Methodology

Our office has a specific set of procedures we use for collecting and analyzing the data in each year's Data Breach Report. These procedures include five specific phases: Acquisition, Evaluation, Scrubbing, Confirmation, and Analysis.

Acquisition

Data is acquired through a high-level review of breach notices submitted to our office. A list of all data breach notices that have been sent to our office since 2015 is publicly available at: https://www.atg.wa.gov/data-breach-notifications.

For each year's report, we looked at all breaches submitted over the course of a year, starting on July 24. For this year's report, that means we looked at all breaches submitted to the Attorney General's Office from July 24, 2019 thru July 23, 2020. The reason for the July 24 start date is that HB 1078 (RCW 19.255.010 and RCW 42.56.590) went into effect on July 24, 2015, requiring breached entities to report data breach notices to the Attorney General when 500 or more Washingtonians are affected.

Evaluation

For the purposes of our report, we only include data from notices that are **required by law** to be sent to our office. For an in-depth description of Washington's Data Breach Notification law, please see the "Washington's Data Breach & Data Security Laws" section on page 21.

For each notice, we assess the information provided against the definition of "personal information" set out in RCW 19.255.005 and RCW 42.56.590, as well as the guidelines for reporting breaches to our office, to determine if they qualify for inclusion in the final dataset.

For example, if our office receives a data breach notice that impacts fewer than 500 Washingtonians, or does not impact any of the elements defined by the law as "personal information," we do not include the breach in our report's dataset. With that said, these notices are still listed on our website for public consumption, and are recorded internally in a separate dataset as "non-qualifying" breaches.

Scrubbing

From time to time, the notices sent to our office do not provide complete information about the nature of the breach. This can occur for various reasons. When this does occur, representatives in our Consumer Protection Division reach out to the notifying entity to try and acquire the missing data. Once obtained, the notice is re-evaluated, and added to either the "qualifying" or "non-qualifying" dataset.

Confirmation

The confirmation phase is an internal process focused on ensuring the quality of the data input into the dataset and the resulting statistics that are generated. This is achieved by reviewing each entry in the dataset to ensure there are no input errors (e.g. putting text in a field where we'd expect numbers), and double checking that the formulas are producing the expected output using "dummy" data entries or other control methods.

Analysis

In this final phase, we calculate our "final statistics" to be represented in the report. These statistics inform the final written analysis of the report, as well as the relevant charts and infographics. This final step can only occur once we have ferried every notice through the first four steps. Once complete, the resulting dataset is given to a second analyst for auditing to ensure the data has been properly calculated.

Impacts from the March 1, 2020 Update to the Data Breach Notification Law

The expansion of our state's law on March 1, 2020 made assembling this year's dataset particularly complex, as the rules for including a notice in the dataset changed half way through the evaluation period. That means that for all notices received between July 24, 2019 and February 29, 2020, we applied the previous iteration of the law that had a narrower definition of "personal information." Conversely, any notice provided after March 1, 2020 was evaluated against the updated law.

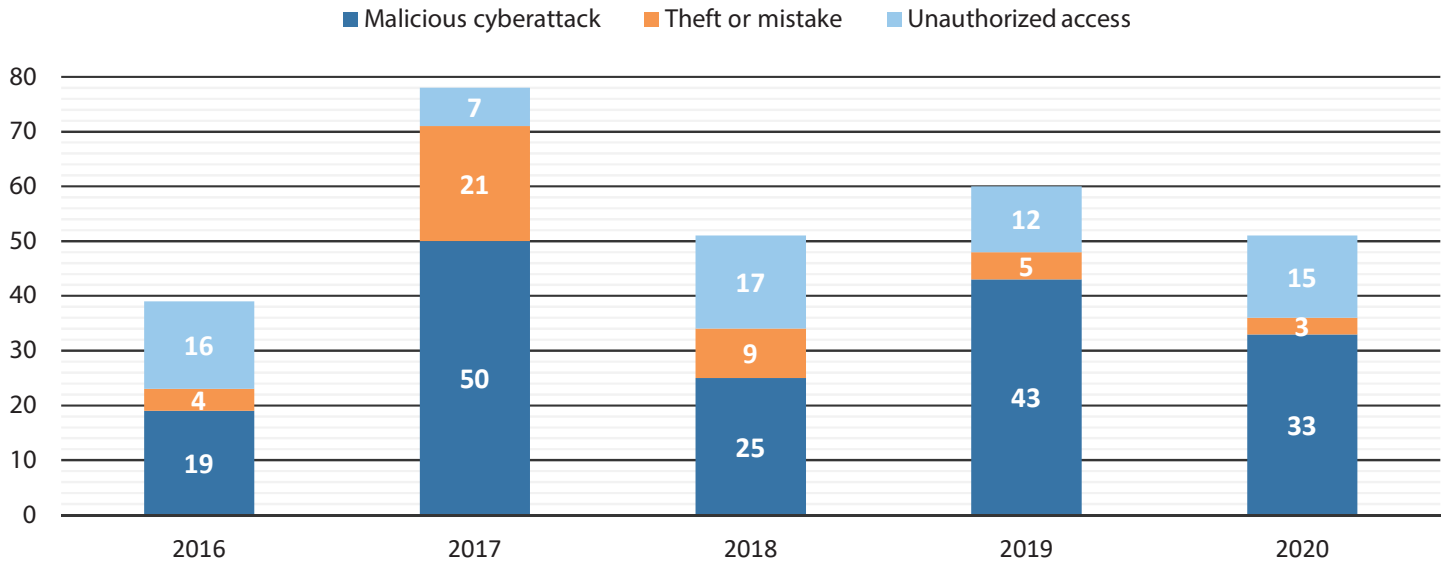
We took this approach in order to stay consistent with our methodology from previous reports. This will allow a fairer comparison between the data collected in previous reports, including trying to understand trends across multiple years.

An example of how this year's dataset was impacted can be seen by looking at two breaches that would not have qualified under the previous iteration of the law. Specifically, a June 10, 2020 notice from Zoosk and a July 10, 2020 notice from Fetch Rewards, Inc. have been included in the dataset, as these breaches included impacted elements like email and password, and date of birth, which became part of the definition of "personal information" in March 2020. Combined, these two breaches represent nearly 250,000 impacted Washingtonians that would have been left out of our dataset in previous years.

These examples clearly illustrate why the update to Washington's Data Breach Notification law in the 2019 session was so critical. Subsequently, the updated law will also allow our office to give a more accurate picture of the impact of data breaches going forward, as we should capture more data than ever before in future Data Breach Reports.

Causes of Data Breaches

Total Number of Data Breaches by Cause



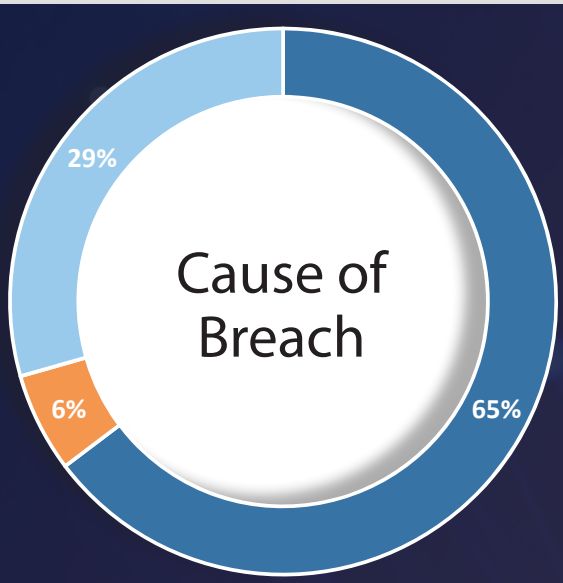
The causes of data breaches can be sorted into three broad categories:

1. Malicious 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 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.

- 33 cyberattacks were reported to our office in 2020, representating a decrease from 2019 when 43 cyberattacks were reported.
- 65% of breaches affecting Washingtonians in 2020 were a result of cyberattacks, down from 2019 when about 72% of breaches were caused by cyberattack.



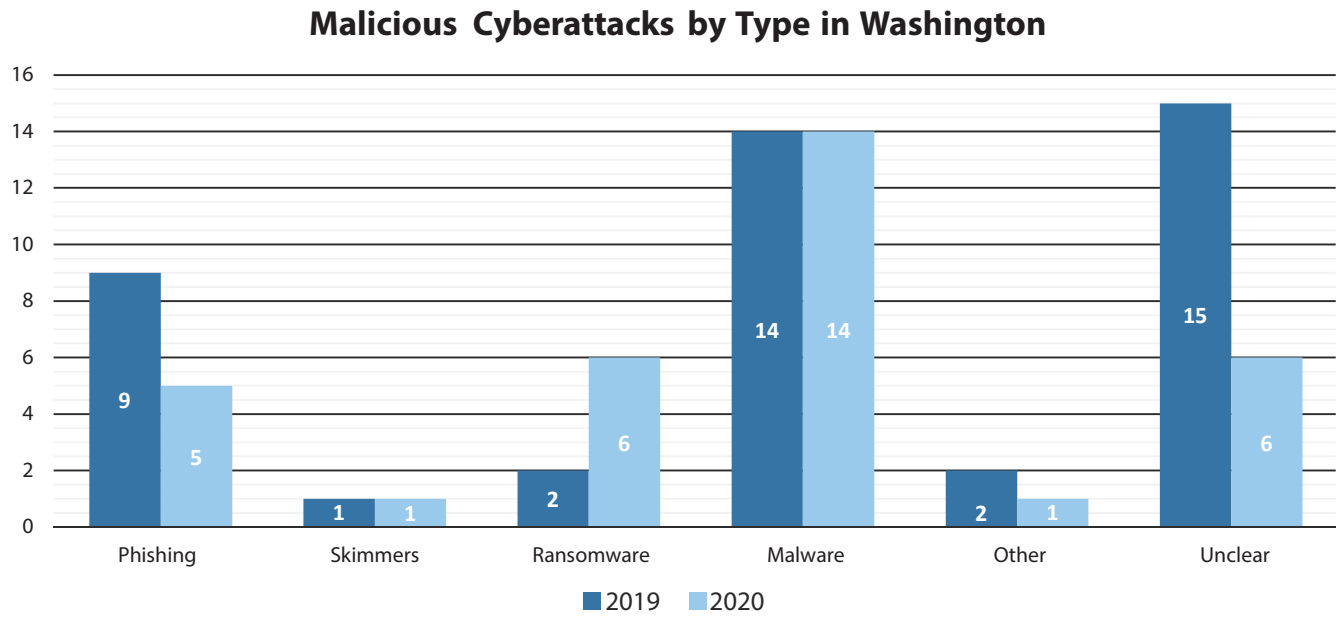
65% - Malicious Cyberattack
6% - Theft or Mistake
29% - Unauthorized Access

A Closer Look at Malicious Cyberattacks

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

- **Malware:** There are various types of malware, but in general, they all revolve around the installation of malicious code onto a website, server, or network in order to disrupt the system, or in the case of spyware, 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. This is typically achieved by inserting 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 an end user 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, the skimmer will be used in conjunction with a device to record PIN information, such as a fake PIN pad or hidden camera.

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



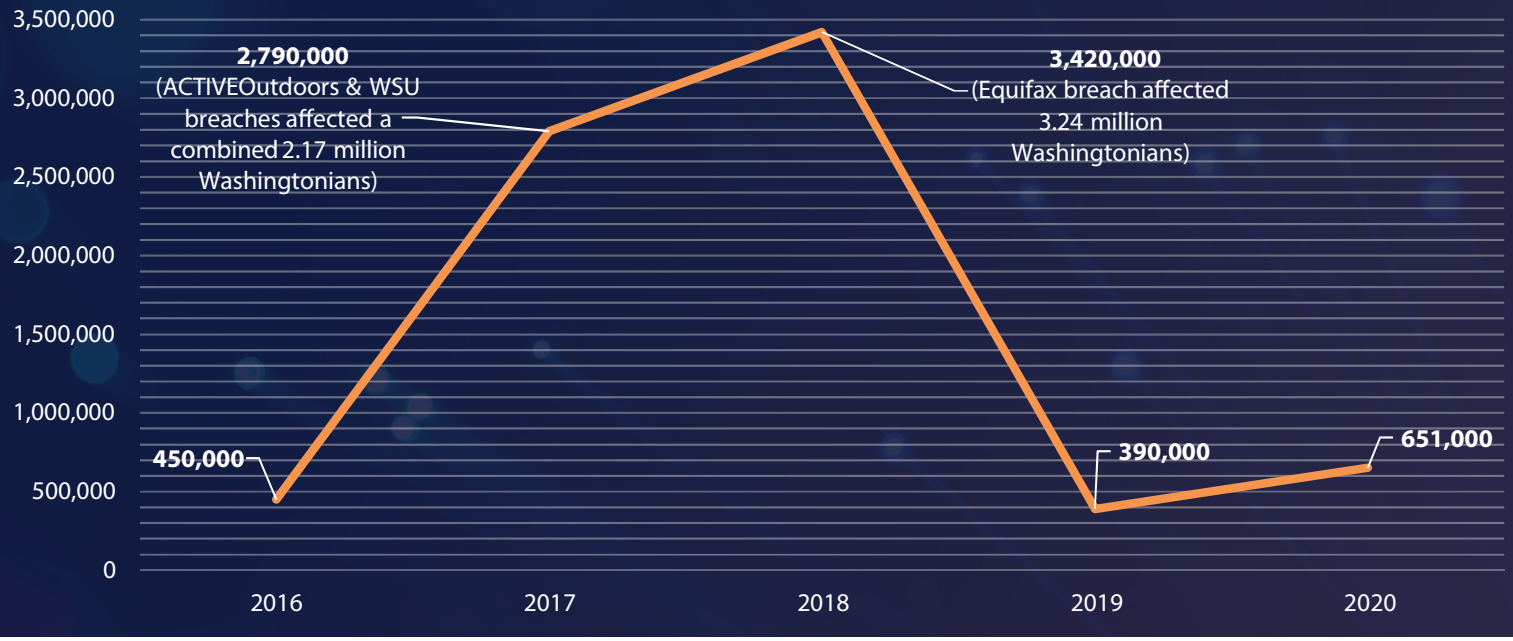
Our office was notified of 33 breaches caused by malicious cyberattacks in 2020. Of those 33 breaches, 6 of the notices did not provide enough information to discern the specific method of cyberattack that was used.

For the remaining 27, just over 40% of these cyberattacks were conducted with malware. This is particularly of concern because malware—and spyware specifically—can be very challenging to detect and often lead to breaches that can go undetected for a significant amount of time. Also of concern is the rise in ransomware incidents, which tripled compared to 2019.

The larger proportion of malware attacks relative to other types of cyberattacks may also be indicative of a continuing trend we observed last year on the part of cyber criminals toward relying on more covert and sophisticated methods of breaching data.

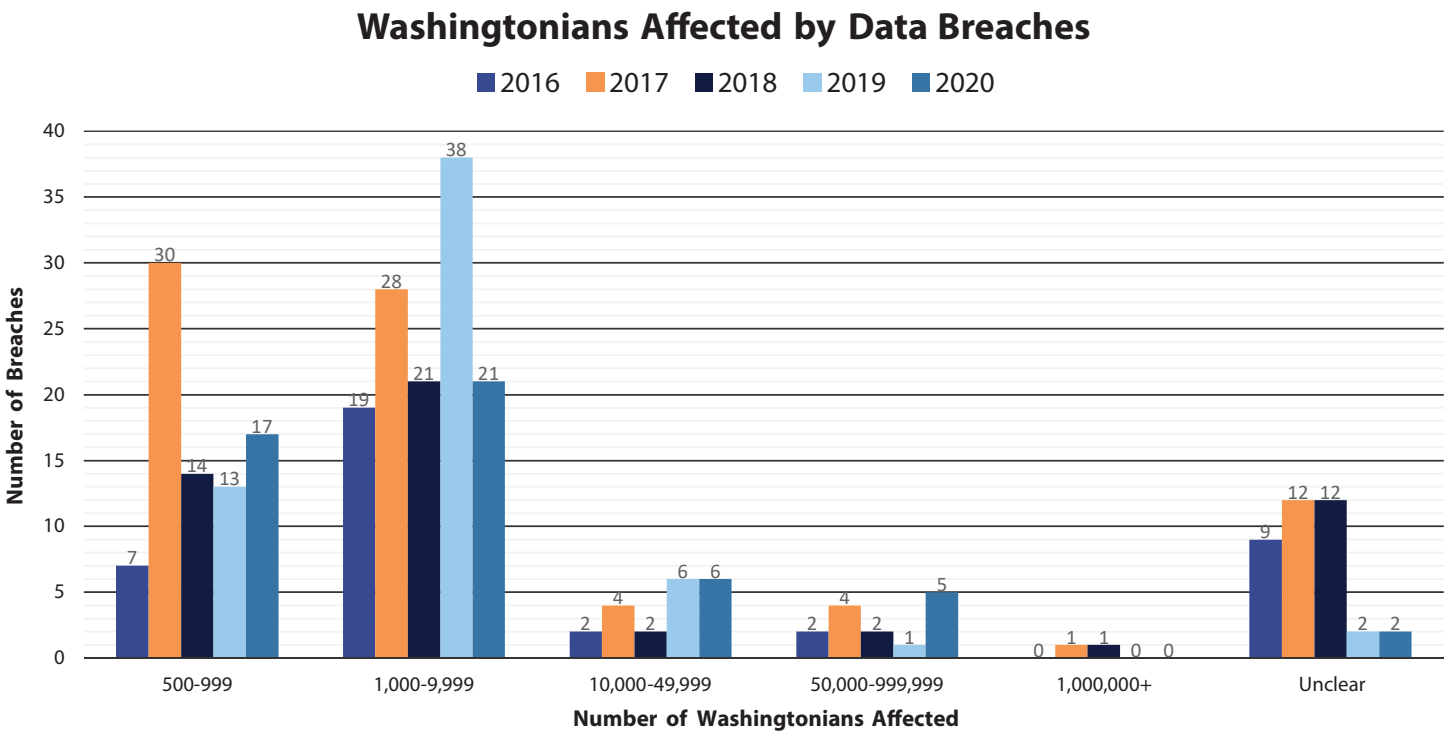
Number of Washingtonians Affected

Annual Number of Washingtonians Affected by Data Breaches Since 2016



In 2020, 51 data breaches affecting more than 500 Washingtonians' personal information were reported to the Attorney General's Office. This is down from 2019's 60 reported breaches. Although the total number of breaches decreased, the total number of Washingtonians affected by these breaches is up 67% from last year, from 390,000 in 2019 to approximately 651,000 in 2020.

This increase is attributable to the fact that our office was notified of five breaches impacting more than 50,000 Washingtonians, compared to only one such breach in 2019. This matches the spike we saw in 2017, where five such breaches also occurred, and slightly above 2018, where three such breaches occurred, including the Equifax mega breach, which affected 3.2 million Washingtonians.

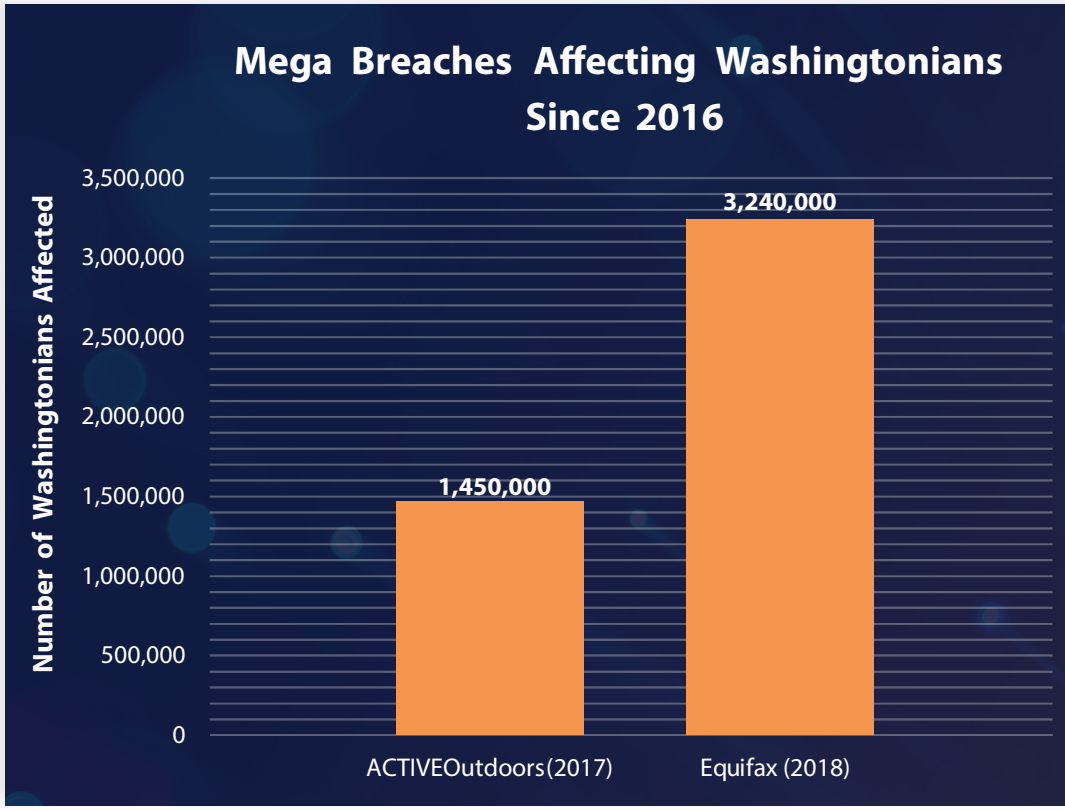


The majority of data breaches reported to our office in 2020 compromised the personal information of between 1,000 and 9,999 Washington residents. This is the third straight year that a majority of breaches have affected at least 1,000 Washingtonians. 2019 marked the highest number of breaches affecting between 1,000 – 9,999 Washington residents since our office started tracking this data, at 38 breaches. While we saw noticeably fewer breaches in this category in 2020 compared to 2019, it still remained the most common with 21 breaches.

What are "Mega Breaches"?

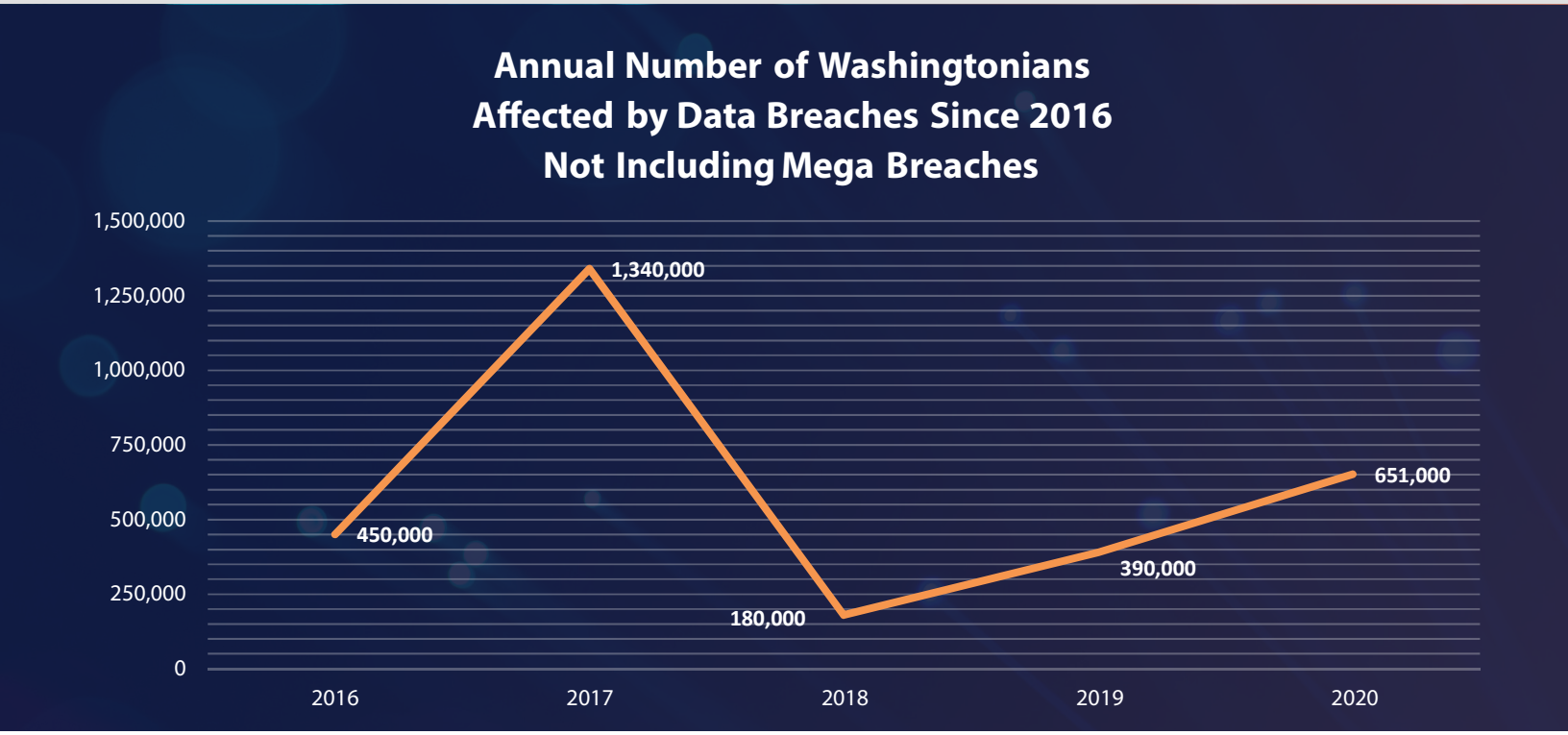
For the purposes of this report, a mega breach is any breach that affects the personal information of 1 million or more Washington residents. These breaches have a tremendous impact on the total number of Washingtonians impacted by data breaches each year, often impacting more people in a single breach than all other breaches from a single year combined.

Since our office began issuing this report in 2016, we have been notified of two confirmed mega breaches – the ACTIVEOutdoors breach in 2017, and the Equifax Breach in 2018.



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 2020 "Cost of a Data Breach Report," breaches compromising 1 to 10 million records cost breached entities an average of $50 million per breach, while breaches affecting more than 50 million records cost an average of $392 million.[8]

Due to their massive size, mega breaches also obscure trend data for the much more common small to mid-size 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 more than doubled in 2019 and continued to grow by an additional 67% in 2020.

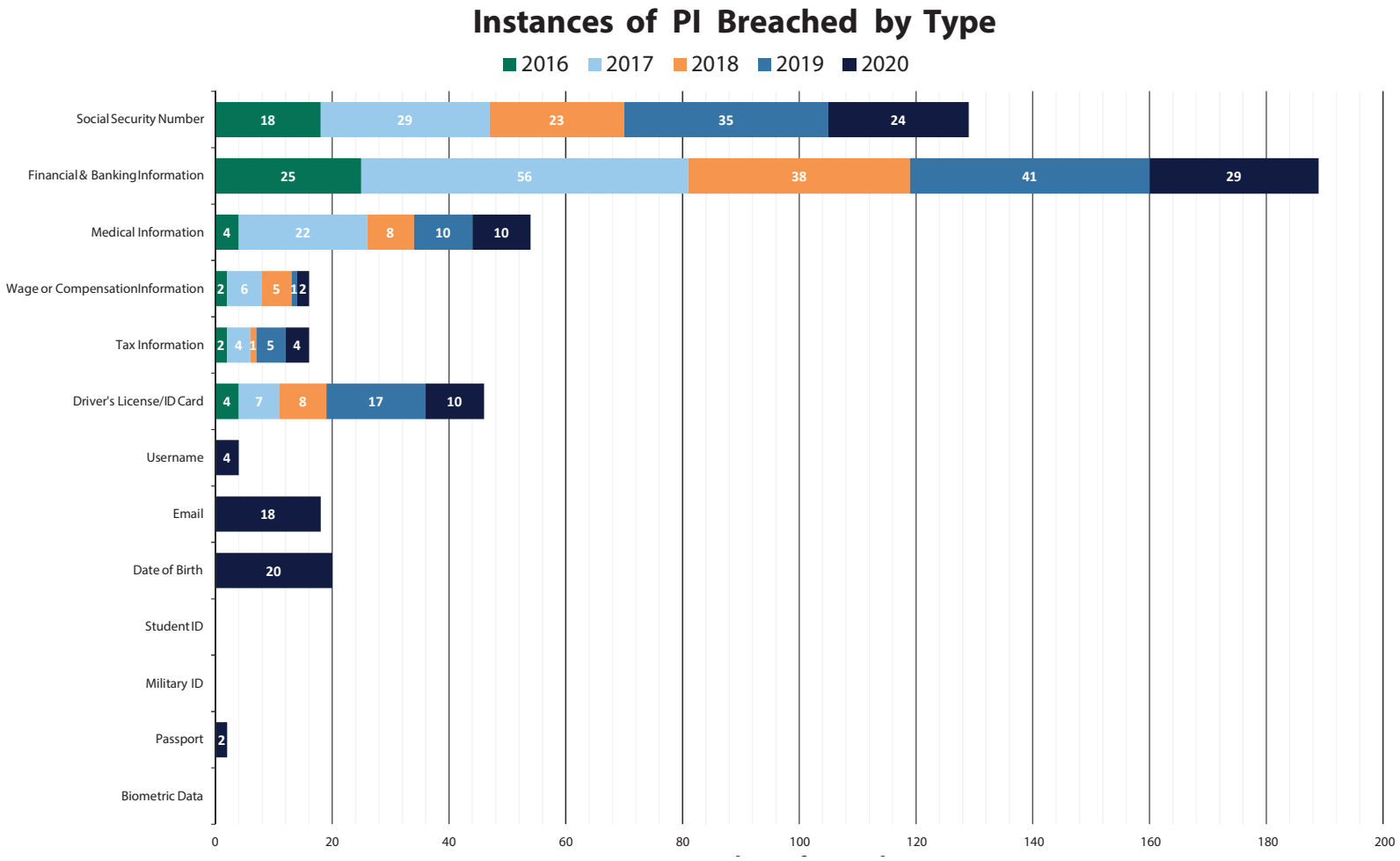
While mega breaches understandably garner a significant amount of attention, it is important that we avoid becoming desensitized to the occurrence of small and mid-size breaches that, cumulatively, impact a significant number of people each year.

Types of Personal Information Compromised

Washington law requires notification to the Attorney General's Office when a data breach includes personal information (PI). Under the current definition of PI in Washington State, this data includes an individual's first name or first initial and last name in combination with any of the following:[9]

- **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.



Note: Username, Email, Date of Birth, Student ID, Military ID, Passport, and Biometric Data were all added to Washington's definition of "personal information" on March 1, 2020. As a result, there is no data for these elements prior to that date.

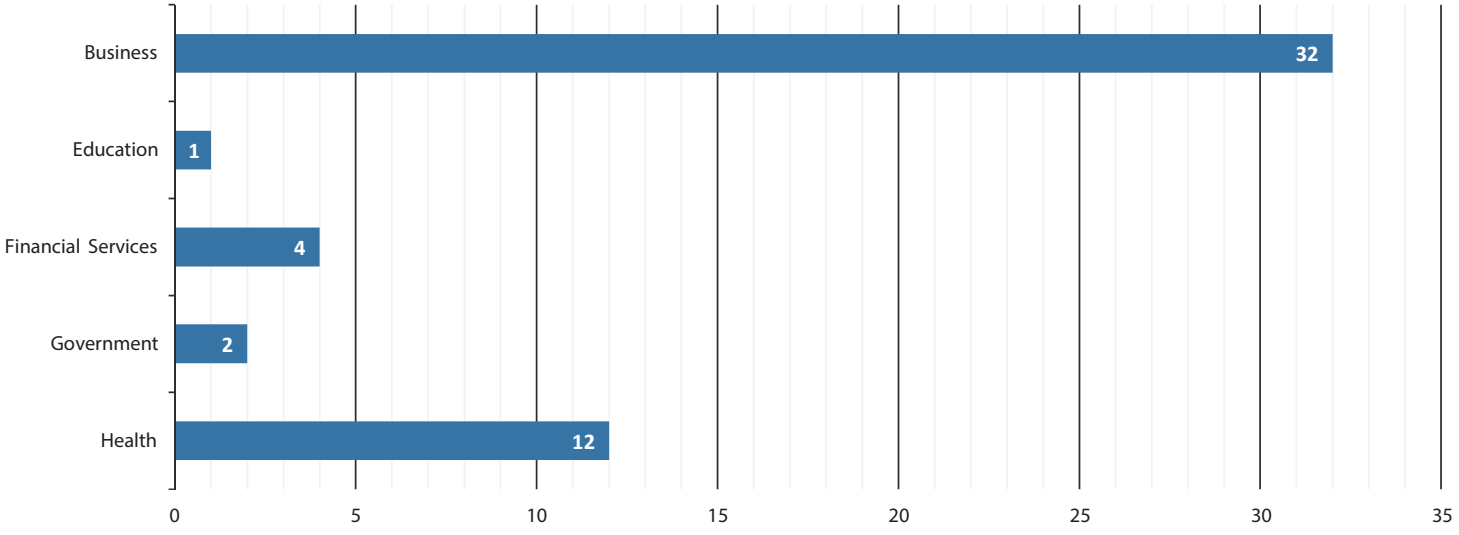
Lastly, any username or email address in combination with a password or security questions and answers that would permit access to an online account are also considered personal information.

In 2020, 29 breaches, representing over half (57%) of all breaches reported to our office this year, resulted in the compromise of some form of financial data. In most cases, this information included the breach of credit or debit card numbers in combination with a security code (e.g. CVV). This is the fifth straight year in which financial information was the most commonly compromised type of personal information.

Consistent with previous years, Social Security numbers came in second, with reported impacts in 47% of breaches. Of the new elements added to the definition of personal information in 2020, date of birth and email in combination with a password were the most prevalent, constituting 39% and 35% of breaches, respectively.

Industries Reporting Breaches

Number of Breaches in 2020 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

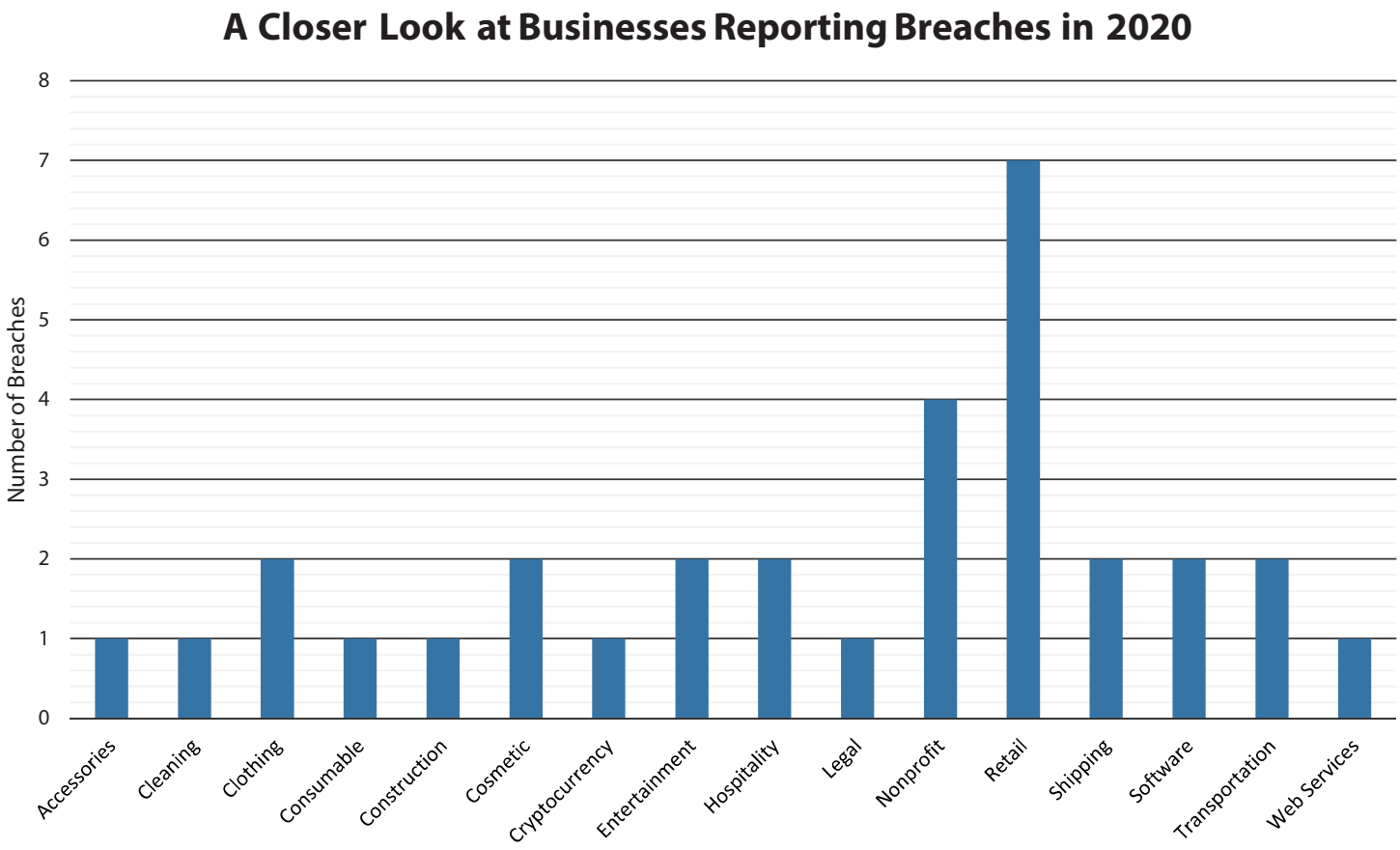
Financial Services

Government

Health Care

The business category includes 24 sub-categories, including retail, nonprofit, transportation, human resources, hospitality, and software.

For a third straight year, the majority of breaches reported in 2020 came from organizations categorized as businesses, which accounted for nearly 63% of all breaches. Malicious cyberattacks were responsible for approximately 60% of these data breaches, with about 63% of these malicious cyberattacks perpetrated through the use of malware, such as having malicious code installed onto servers or websites.



Within the business category, the retail (21.8%) and nonprofit (12.5%) sub-categories were the most common types of businesses to be breached, representing a third of all breaches reported to our office by businesses in 2020.

In addition to being the most frequently breached industry in 2020, the business category also had the largest total number of affected Washingtonians. Breaches of businesses in 2020 affected on average 16,759 Washingtonians per breach, and accounted for approximately 77% of all Washingtonians impacted by data breaches in 2020. This is up significantly from 2019, when breaches impacting businesses affected on average 3,831 Washingtonians, accounting for 35% of all Washingtonians impacted by breaches in 2019.

Impact of Data Breaches on Washington Businesses

Under Washington law, businesses have a responsibility to take reasonable steps to protect the security of individuals' personal information. The variety of ways that data breaches can occur – including inadvertent disclosure, theft of hard copy information, and malicious cyberattacks – create risks for all businesses.

According to the Ponemon Report, the average cost of a data breach in the United States in 2020 is $8.6 million, up 5% from 2019.[10] The study also found that on average breaches in the United States were more expensive than anywhere else in the world, and significantly higher than the global average of $3.86 million per breach.

The study also found that, globally, malicious attacks remain the primary cause of data breaches – approximately 52% of the cases studied in 2020 – and are still the most expensive type of data breach for businesses. According to the report, breaches caused by a malicious attack cost an average of $4.27 million globally, compared to $3.3 million globally for breaches caused by a system glitch or human error.

With the costs of data breaches continuing to rise it is clear that the threat of malicious cyberattacks will continue to be a major threat to Washington businesses and their consumers for the forseeable future. It also underscores the importance of businesses planning for and being prepared to address a breach of their records.

The Ponemon Report notes that businesses that had an incident response team and extensive testing of their response plans prior to a breach saved on average $2 million per breach in 2020, compared to businesses that took neither of these steps.

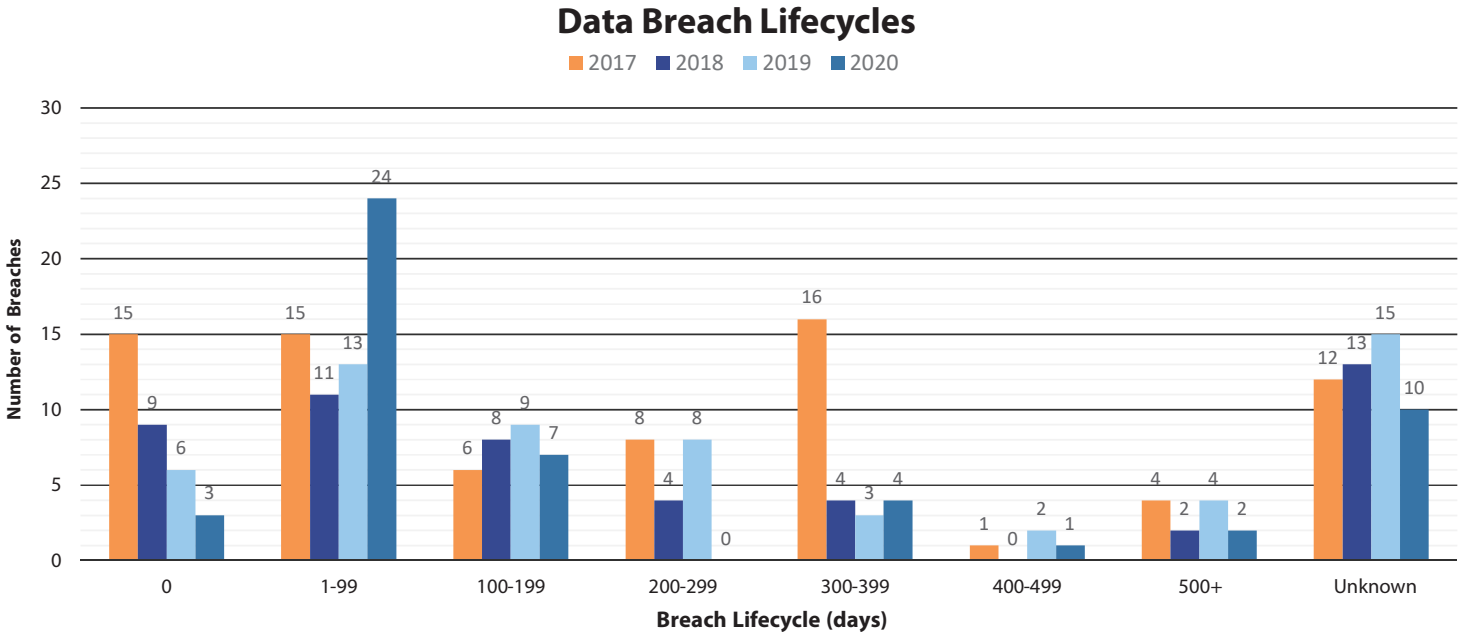
Time to Resolve Data Breaches

What is a Breach's "Lifecycle"?

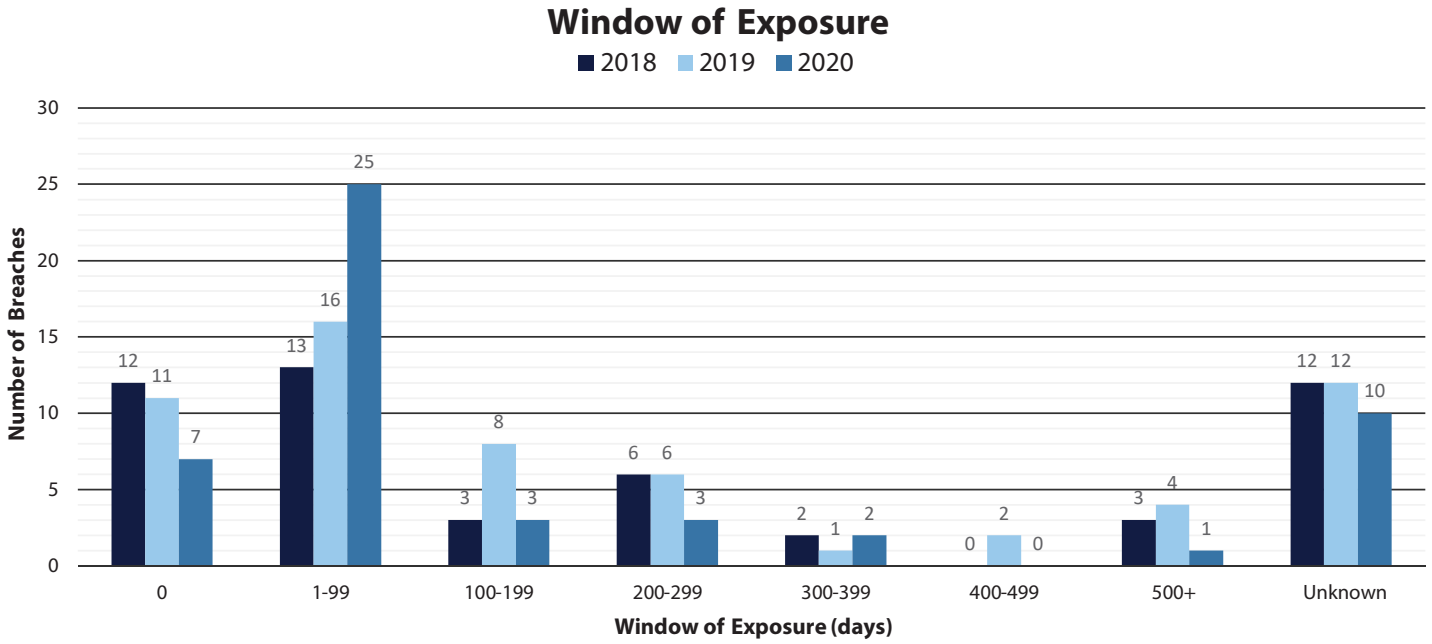
Resolution of a breach involves two steps:

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

In this report, identification is measured as the number of days that pass between the start of the breach and its discovery by the affected organization. Containment is represented by the number of days that pass between discovering the breach and securing access to the compromised information. The total time to resolve a data breach is the sum of these two measurements. This is referred to as the "lifecycle" of a breach.



This is not to be confused with the period of time in which a breach is active, also known as the "window of exposure." Sometimes the theft of information concludes before it is discovered by the breached entity. This was the case in 12 (29%) of the breaches reported to the Attorney General's Office in 2020. 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.



A example of this can be found in a breach that was reported to our office by Creation Entertainment, Inc. (CEI) on August 26, 2019. In this case, CEI reported that they had discovered evidence of, "suspicious activity surrounding credit and debit card numbers" between February 1, 2018 and October 10, 2018. This represents a window of exposure of approximately 250 days.

However, representatives at CEI did not become aware of the possibility that a breach had occurred until March 18, 2019 – 410 days after the breach began. As a result, the lifecycle of this breach (410 days) was longer than the window of exposure (250 days). Breaches with long life cycles are of particular concern because they leave consumers uninformed of the risk to their information for a significant period of time.

The majority of data breaches reported in 2020 had both a window of exposure and lifecycle of less than 100 days. On average, breaches with a lifecycle of 1 to 99 days affected 13,429 Washingtonians per breach in 2020.

There were also a significant number of breaches in 2020 where the window of exposure or lifecycle could not be determined from the notification provided to our office, categorized as "Unknown." In 2020, there were 10 cases where the lifecycle of the breach could not be determined. On average, these incidents affected 16,354 Washingtonians per breach.

The Average Lifecycle of Breaches by Industry

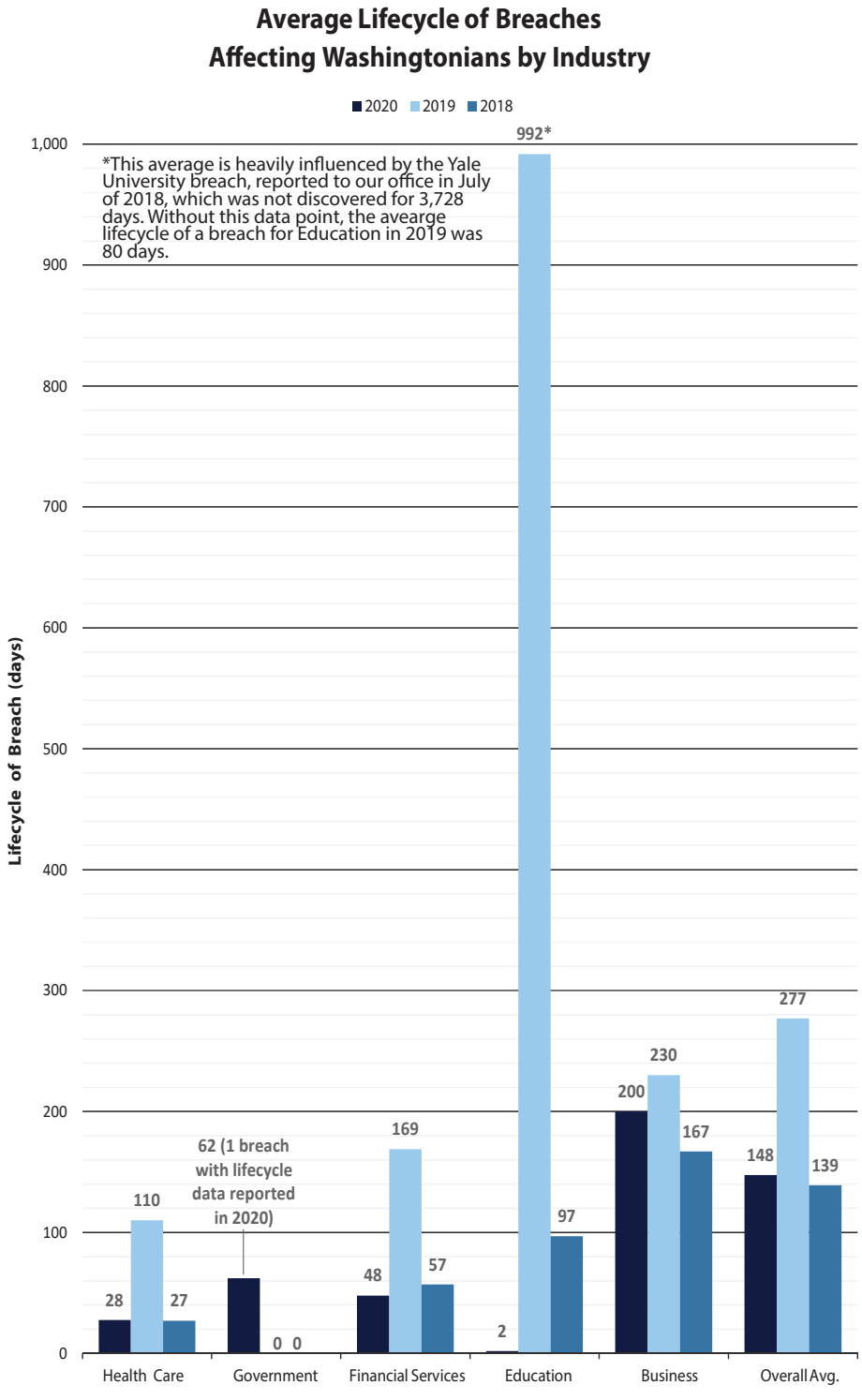
The average lifecycle of a breach decreased for all industries in 2020, with the exception of Government. However, it should be noted that the increase to the Government average is the result of a single data breach reported in November 2019. In the previous two years, there were no qualifying breaches reported to our office from any Government entities.

On average, breaches reported to the Attorney General's Office had a lifecycle of 148 days, a 47% decrease from 2019 when the average was 277 days.

The decrease in lifecycle length in 2020 is more in line with the average lifecycle we saw in 2018 of 139 days. This indicates that 2019 may have been an outlier, largely driven by a major jump in the time it took organizations to discover breaches after they occurred – from an average of 135 days in 2018, to 330 days in 2019. In 2020, that number came back down to 123 days.

In the 2019 Data Breach Report, we considerd the possibility that the lifecycle averages in 2019 might prove to be an outlier in the longrun. That theory was driven by the fact that in 2019 there were two breaches that significantly impacted the data, including a breach at Yale University, which took over 3,000 days to discover. With those two data points removed, the average time to discover a breach in 2019 came in at a more typical 192 days – although still a 42% increase from 2018.

Even if 2019's lifecycle data proves to be an outlier, the fact that the average lifecycle of a breach in 2020 remains above 100 days is indicative of the continued difficulty businesses are having detecting breaches as cyber criminals increasingly rely on more complex and covert methods of breaching security systems.



How Long Did Businesses Take to Resolve Breaches?

The average lifecycle of a breach was longer for businesses than any other industry, with an average of 200 days per breach. This represents a 13% decrease for businesses since 2019's report, when the average was 230 days. Of the 32 businesses reporting data breaches to the Attorney General's Office in 2020, 30 specified the amount of time it took them to identify the data breach. Of those 30 businesses, 18 reported that they had discovered the data breach in fewer than 100 days after it began. Seven businesses (23%) reported a breach with a lifecycle of more than 200 days. That is down from 2019, when 41% of businesses reported breaches with a lifecycle of more than 200 days.

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.[11] Notably, the Ponemon Report also states that the global average lifecycle of a breach across all industries in 2020 was 280 days. For breaches reported to our office, the 2020 average across all industries was 148 days.

Washington's Data Breach & 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 be notified 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 also are considered personal information.

It should also be noted that SB 6187, which was signed by Governor Inslee 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.

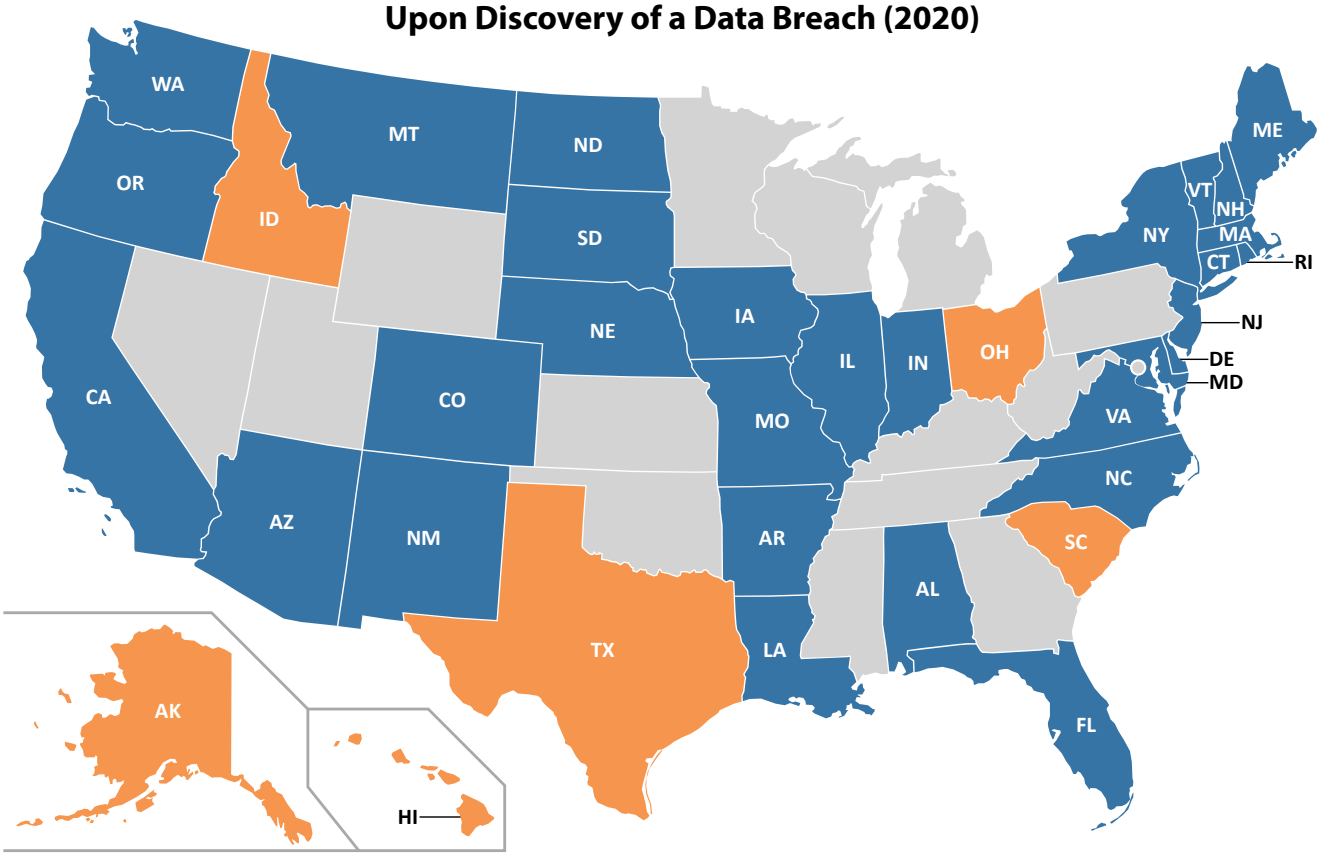
When the entity holding this personal information is covered by the Health Insurance Portability and Accountability Act (HIPAA) the entity must provide notification to the Attorney General's Office of a breach. These entities are deemed to comply with the timeliness of the notification requirement as 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 is focused 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.

How Does Washington's Law Compare to Other States?

States Requiring Notification of State Attorney General Upon Discovery of a Data Breach (2020)



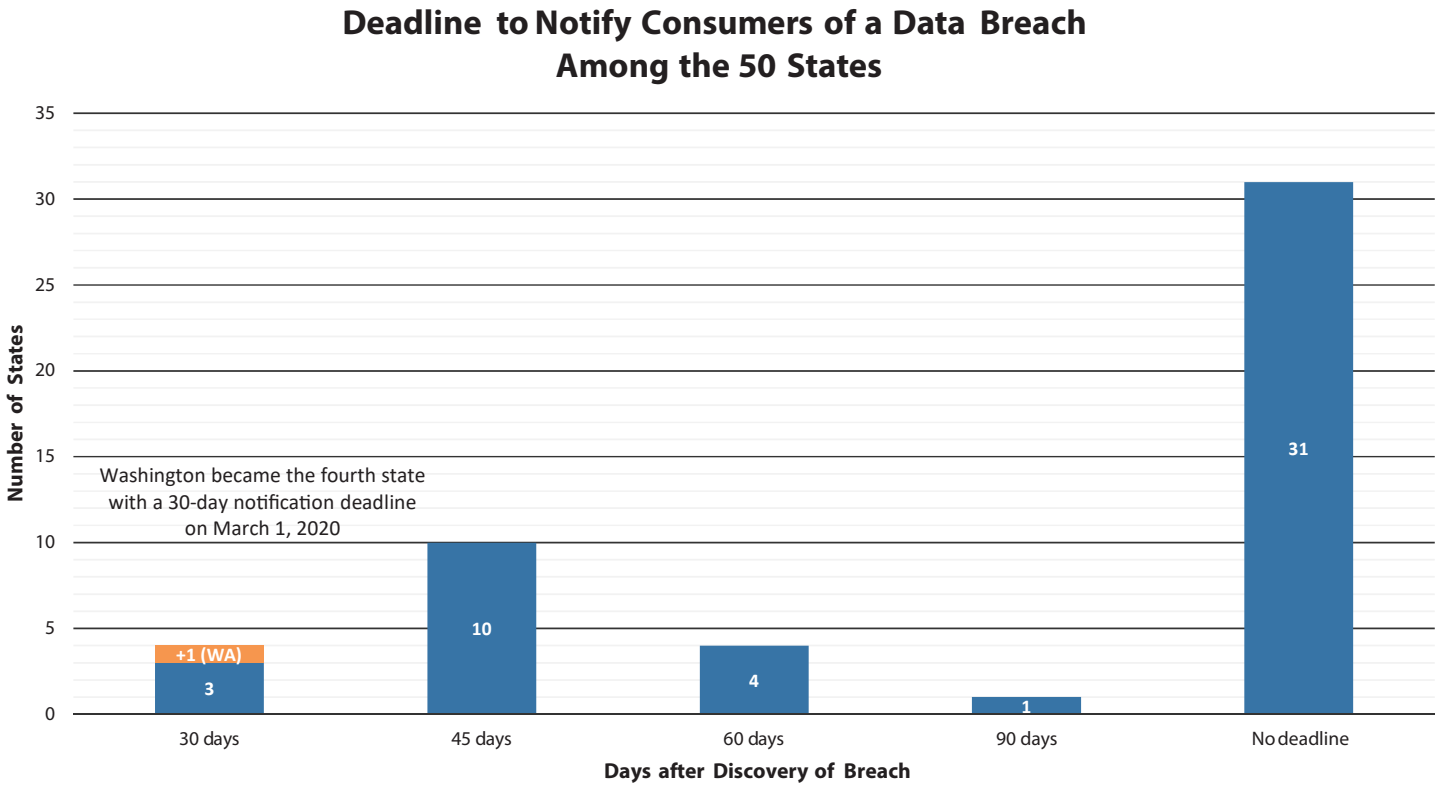
*States in **orange** only require notification to the Attorney General under special circumstances (e.g. Idaho only requires notice from public agencies), and/or require notification to a state agency that is not the Attorney General (e.g. Hawaii requires notice to the Office of Consumer Protection).

Washington Compared to Other States

All 50 states have laws requiring private or governmental entities to notify individuals when a data breach occurs.[12]

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.[13]

In 36 states, including Washington, entities experiencing a breach must notify the Attorney General or another state agency.[14] 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.[15] 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.[16] Unlike Washington, however, neither state has an explicit deadline to notify consumers for breaches affecting private entities.



SOURCE: Perkins Coie. (2020, June). "Security Breach Notification Chart." Accessed September 2020, from https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

In fact, only 19 states, including Washington, have a specific deadline for reporting breaches to consumers.[17] As of September 2020, 4 states, including Washington, have a 30 day deadline to notify consumers. Along with Florida, Colorado, and Maine, this represents the shortest deadline to notify consumers in the country.

Most states with a deadline, including Washington (RCW 19.255.010 (16)), are triggered upon the 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

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
E-mail 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

SOURCE: Perkins Coie. (2020, June). "Security Breach Notification Chart." Accessed September 2020, from https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

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. 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 were not considered 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.

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 account 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.[18]

Massachusetts' law, conversely, requires names to be part of the breach of financial information to trigger notice, but not passwords or security codes.[19] Nuances like this exist for other data elements as well, such as Indiana's notification law, which can be triggered if an individual's Social Security number is breached, even if the name of the associated individual is not.[20]

Washington has among the strongest notification statutes, including the required 30-day notification, as well as one of the most comprehensive definitions of PI.

At the time of publication Washington's law stands out as defining more elements of personal information than any other state (15), providing Washingtonians with one of the most robust Data Breach Notification laws in the country. This, in combination with being one of four states with the shortest deadline for consumer notice (30 days), and one of the only states who continue 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 (page 21).

Conclusion & Recommendations

Data breaches continue to be a significant concern for Washingtonians in 2020 and beyond. Despite the decrease in the total number of breaches reported to our office from 2019, the total number of Washingtonians impacted by breaches increased by 67% this year. The growing number of Washingtonians affected by breaches this year further highlights the importance of the data breach 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 for a greater variety of their data in 2020. In short, Washington now has one of the most robust data breach laws in the nation.

However, even with these important updates, opportunities remain for policymakers to continue strengthening our state's laws protecting the personal information of Washingtonians. Potential improvements include:

1. **Bring RCW 19.255.005 and RCW 42.56.590 into alignment by making sure that private entities also have to provide notice to consumers for breaches of a consumer's name and the last-four digits of their Social Security number.**

SB 6187, which was signed by Governor Inslee 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 SSN in combination with a consumer's name as a stand alone element that will trigger the requirement for consumer notice. This change should be extended 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. **Expand the definition of "personal information" in RCW 19.255.005 and RCW 42.56.590 to include Individual Tax Identification numbers (ITINs).**

ITINs are assigned by the IRS 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, ten 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.[21]

3. **Establish a legal requirement for persons or businesses that store personal information to maintain a risk-based information security program, and to ensure that information is not retained for a period longer than is reasonably required.**

As this report discussed last year, it is imperative that entities who handle the private information of Washingtonians take steps necessary to keep it safe, and be prepared to act if they cannot. Such precautions are beneficial for both consumers and the organizations collecting their data. In 2019, Ponemon Report indicated that 48% of the companies surveyed lacked any form of security automation – security technologies used to detect breaches more efficiently than humans can.[22] In 2020, that number dropped by only 7%.[23]

In 2019, the average cost of a data breach for companies without automation was nearly twice as expensive as for those who implemented security automation.[24] That cost has only grown since, with data breaches in 2020 costing companies without security automation nearly triple that of business who have automation. Similarly, the formation of a dedicated Incident Response Team and testing of an Incident Response Plan reduced the average total cost of breaches in 2020 by more than $2 million.[25]

Requiring data collectors to maintain an appropriately sized security program and incident response team and to dispose of consumer information that is no longer needed is a critical next step in mitigating the size and cost of breaches in our state.

Resources for Individuals & Businesses

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 will not be compromised. If you receive a data 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

All organizations that are entrusted with individuals' information are potentially susceptible to data breaches. 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 http://www.atg.wa.gov/identity-theft-and-privacy-guide-businesses.

An FAQ providing specific information about the March update to our state's data breach laws can also be found 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 needed. 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 including developing a dedicated Incident Response Team, or implementing automated security technologies to detect attempted breaches. Page 68 of the 2020 Ponemon Report provides more detail on these steps, and others. You can find the report for download here: https://www.ibm.com/security/digital-assets/cost-data-breach-report/.

Notes

1 TechRepublic. Bayern, M. (2020, June 23). "Only 31% of Americans concerned with data security, despite 400% rise in cyberattacks." Accessed September 2020, from https://www.techrepublic.com/article/only-31-of-americans-concerned-with-data-security-despite-400-rise-in-cyberattacks/.

2 How-To Geek. Hoffman, C. (2019, March 26). "What is a "Dark Web Scan" and Should You Use One?" Accessed September 2020, from https://www.howtogeek.com/394427/what-is-a-dark-web-scan-and-should-you-use-one/.

3 NBC News. Kaplan, E. & Collier, K. (2020, April 14). "Passwords and email addresses for thousands of Zoom accounts are for sale on the dark web" Accessed September 2020, from https://www.nbcnews.com/tech/security/passwords-email-addresses-thousands-zoom-accounts-are-sale-dark-web-n1183796.

4 Ibid.

5 How-To Geek. Hoffman, C. (2019, March 26). "What is a "Dark Web Scan" and Should You Use One?" Accessed September 2020, from https://www.howtogeek.com/394427/what-is-a-dark-web-scan-and-should-you-use-one/; NBC News. Weisbaum, H. (2019, February 4). "You've been breached: Hackers stole nearly half a billion personal records in 2018", Accessed September 2020, from https://www.nbcnews.com/business/consumer/you-ve-been-breached-hackers-stole-nearly-half-billion-personal-n966496.

6 NBC News. Weisbaum, H. (2019, February 4). "You've been breached: Hackers stole nearly half a billion personal records in 2018." Accessed September 2020, from https://www.nbcnews.com/business/consumer/you-ve-been-breached-hackers-stole-nearly-half-billion-personal-n966496.

7 Washington State Employment Security Department. (2020, May 18). "Update on imposter fraud from Commissioner Suzi LeVine." Accessed September 2020, from https://esd.wa.gov/newsroom/update-on-imposter-fraud.

8 Ponemon Institute. (2020, July). "2020 Cost of a Data Breach Report."

9 RCW 19.255.010, effective since March 2020.

10 Ponemon Institute. (2020, July). "2020 Cost of a Data Breach Report."

11 Ibid.

12 Perkins Coie. (2020, June). "Security Breach Notification Chart." Accessed September 2020, from https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

13 Ibid.

14 Ibid.

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

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

17 Perkins Coie. (2020, June). "Security Breach Notification Chart." Accessed September 2020, from https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

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

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

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

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

22 Ponemon Institute. (2019, July). "2019 Cost of a Data Breach Report."

23 Ponemon Institute. (2020, July). "2020 Cost of a Data Breach Report."

24 Ponemon Institute. (2019, July). "2019 Cost of a Data Breach Report."

25 Ponemon Institute. (2020, July). "2020 Cost of a Data Breach Report."