Washington State
Attorney General's Office

2019
Data Breach Report

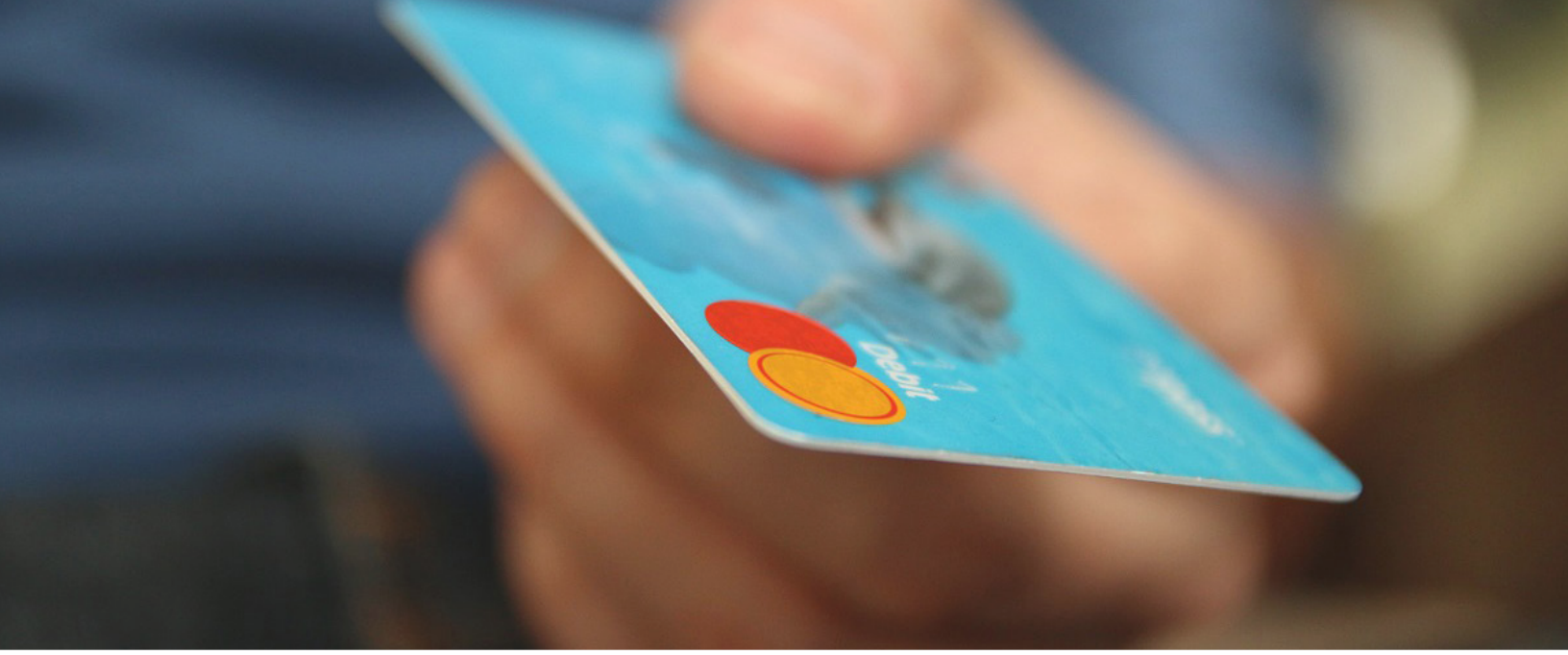


Table of Contents

Letter from Attorney General Bob Ferguson

October 2019

Dear Washingtonians,

Data breaches are a significant threat to Washington residents, businesses and agencies. In 2019, the total number of breaches reported to our office increased by nearly 20%, with just over 70% resulting from a malicious cyberattack. The lifecycle of breaches also increased dramatically, rising from an overall average of 139 days in 2018 to 277 days in 2019.

These numbers follow the already alarming trends reported in the 2018 Data Breach Report. In response to those trends, I requested legislation during the 2019 legislative session to strengthen our state's data breach laws. The bill, which unanimously passed both the House and Senate, expands our state's notification requirements to include more types of consumer information and reduces the deadline to notify consumers from 45 to 30 days. As this year's report shows, data breaches remain a serious threat to our privacy, and this law will arm consumers with information to protect their sensitive data. These changes go into effect in March 2020.

My office is also taking action to protect consumers when companies fail to reasonably secure data or provide timely notice to impacted consumers.

In July, after an investigation by 30 states led by my office, Premera Blue Cross agreed to pay $10 million nationwide for their failure to secure consumers' personal information and for misleading consumers before and after a data breach. The breach occurred between May 5, 2014 and March 6, 2015, when a hacker gained access to a Premera network containing more than 10 million individuals' personal information, including that of 6.5 million Washingtonians.

My office also announced in July that credit-reporting agency Equifax will pay up to $425 million in restitution for consumers for its 2017 data breach affecting nearly 150 million consumers nationwide, including 3 million Washingtonians. Equifax will also pay $175 million to the states, including more than $3.7 million to Washington, which will go toward continued enforcement of state data security and privacy laws. Additionally, this resolution requires Equifax to implement an "Information Security Program," which will limit the collection and use of individuals' personal information going forward.

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 45 days of discovering the breach, as well as to 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, legislation strengthening Washington's data breach notification law. This legislation, sponsored by Rep. Shelley Kloba and Sen. Joe Nguyen, significantly expands the definition of "personal information," requires that notices to consumers include the period of time their data was at risk, and reduces the deadline to provide notice to 30 days after the discovery of a breach. These changes go into effect in March 2020, and will give Washington State one of the most robust data breach notification laws in the country.

This 2019 report is based on data breach notifications received by the Attorney General's Office between July 24, 2018 and July 23, 2019 that affected more than 500 Washingtonians' personal information. The data reveals:

- Malicious cyberattacks continue to be the leading cause of data breaches affecting Washingtonians, representing 72% of all breaches reported to our office in 2019. Just over half of these breaches were the result of malware or phishing e-mails.
- The number of Washingtonians affected by breaches decreased significantly in 2019 compared to previous years. In fact, 2019 represented the fewest number of Washingtonians impacted by breaches since the Attorney General began collecting and publishing this data in 2016.
- However, the total number of breaches increased from 51 in 2018 to 60 in 2019.
- Unlike 2017 and 2018, no mega breaches were reported in the period covered by the 2019 report. However, Capital One announced a breach in late July, which affected an estimated 100 million Americans. Consequently, we expect the total number of affected Washingtonians to increase next year.
- Removing "mega breaches" affecting one million or more Washingtonians from the data also shows that the total number of Washingtonians impacted by small to mid-size breaches more than doubled – from 180,000 in 2018 to 390,000 in 2019. Relatedly, for the second year in a row, the majority of

breaches reported to our office affected between 1,000-9,999 Washingtonians. This number grew from 21 such breaches in 2018, to a staggering 38 in 2019.

- For the fourth straight year, financial information was the most commonly compromised type of personal information, affected in 68% of reported breaches, closely followed by Social Security numbers, affected in 58% of reported breaches.

- The lifecycle of breaches increased dramatically, rising from an overall average of 139 days in 2018 to 277 days in 2019. This was largely driven by a huge in spike in the amount of time it took organizations to discover that a breach had occurred.

Recommendations

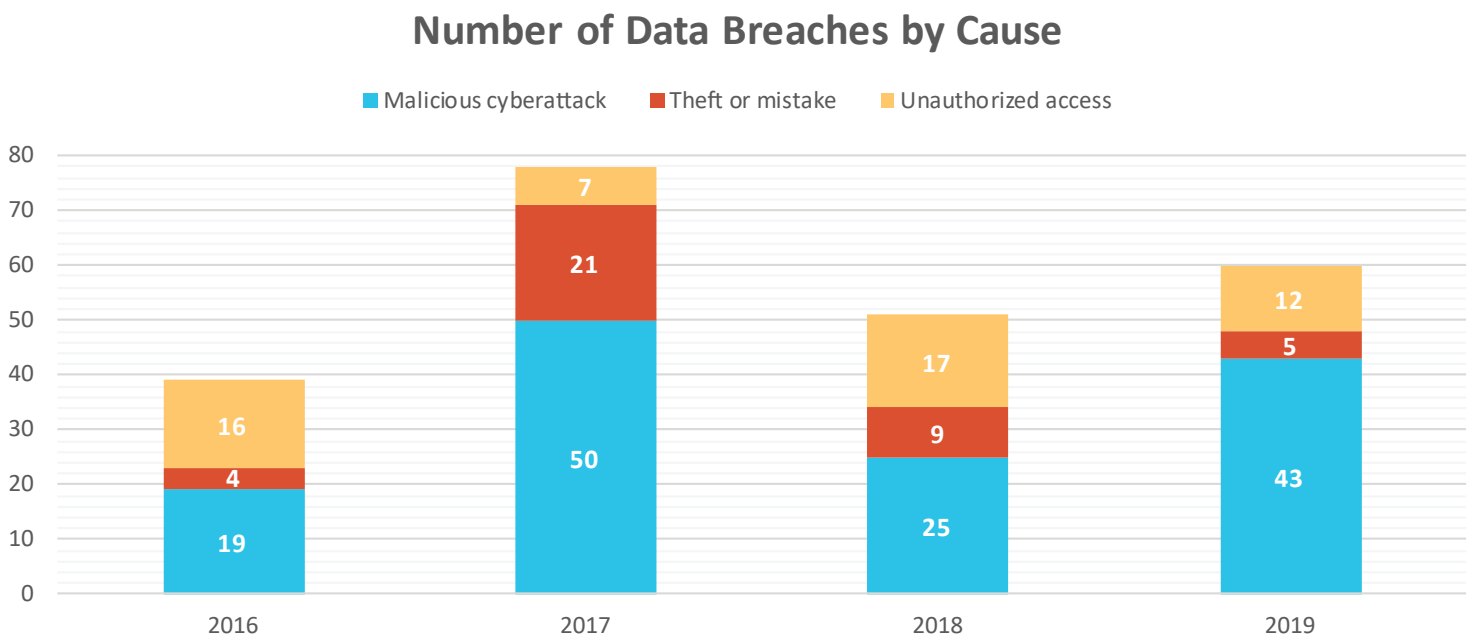
In addition to the important updates coming to our state's data breach notification law in March, opportunities remain for policymakers to continue strengthening our state's laws protecting the personal information of Washingtonians. The Attorney General's Office recommends that policymakers:

1. Expand the definition of "personal information" to include Individual Taxpayer Identification numbers and Tribal ID numbers;

2. Amend the law to require that the breach of financial information and Social Security numbers are standalone triggers for notice to consumers, even if the full names of the associated individuals were not breached; and

3. Require 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.

Causes of Data Breaches



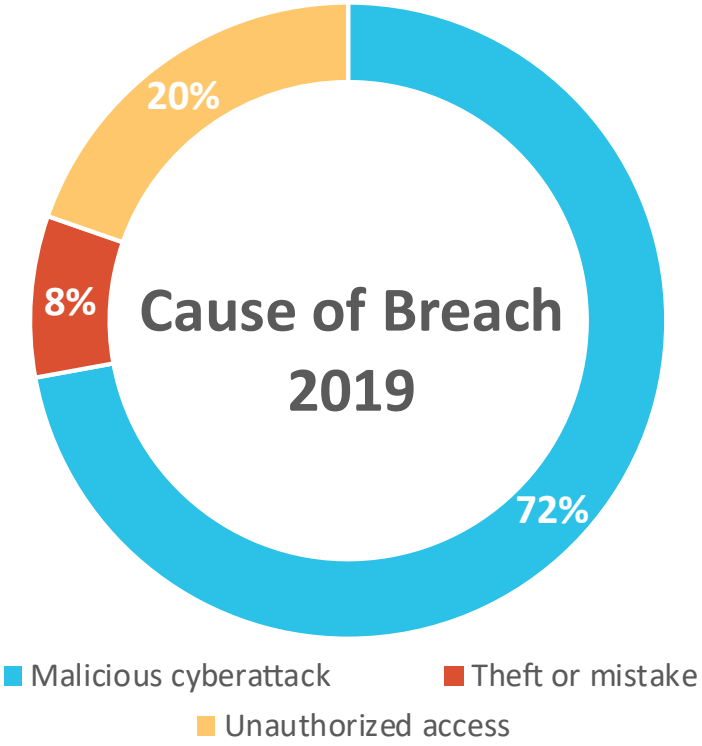
The causes of data breaches can be sorted into three broad categories:

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.

Causes of Data Breaches



- **The total number of cyberattacks in 2019 is nearly double that of 2018, with 43 cyberattacks reported to our office this year.**
- **72% of breaches affecting Washingtonians in 2019 were a result of cyberattacks, up significantly from 2018 when roughly half of breaches were caused by cyberattack.**

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

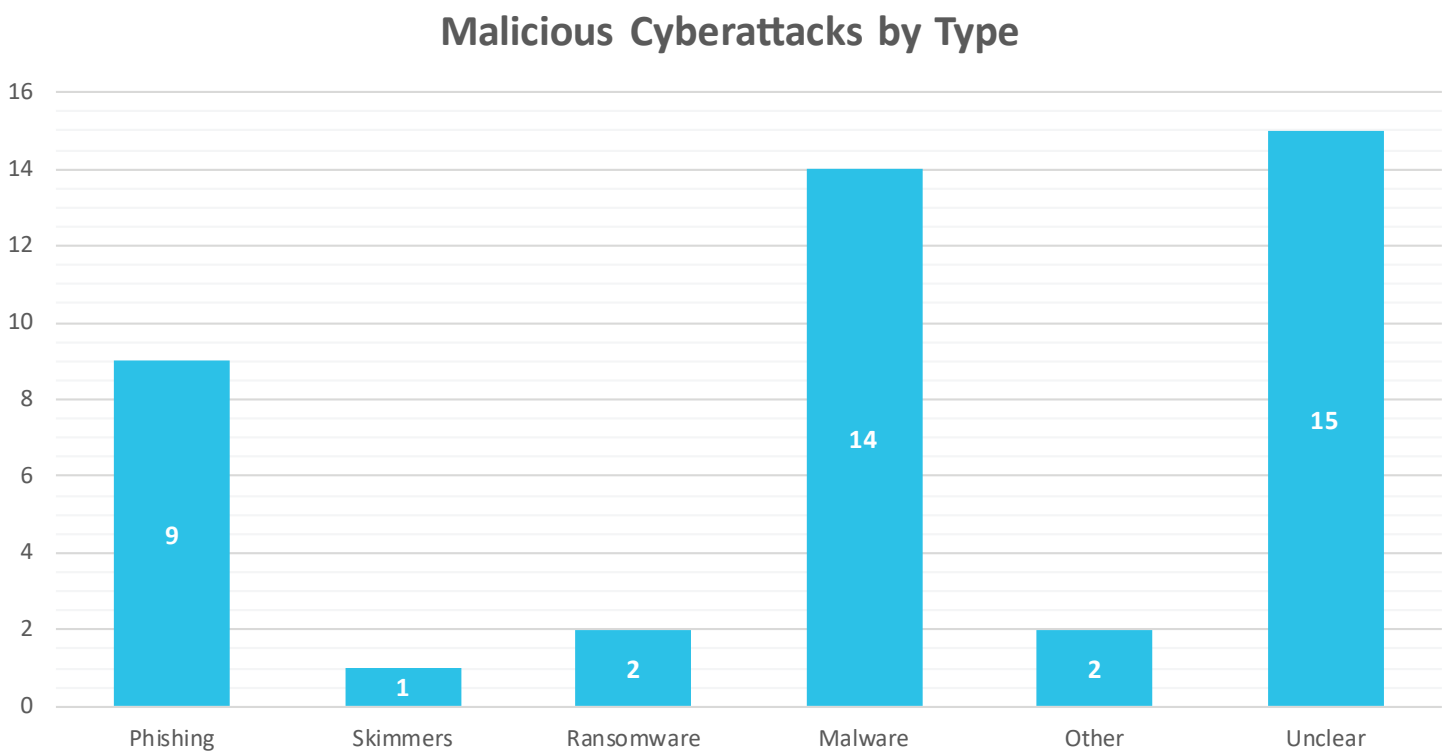
A unique type of malware that holds data hostage in hopes of receiving a ransom payment from the breached entity. This is typically achieved by inserting malicious code into a network that encrypts the data, and thus renders it inaccessible to the breached organization.

Phishing

The practice of sending a fraudulent communication, often times 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.



Our office was notified of 43 breaches caused by malicious cyberattacks in 2019. Of those 43 breaches, 15 of the notices did not provide enough information to discern the specific method of cyberattack that was used.

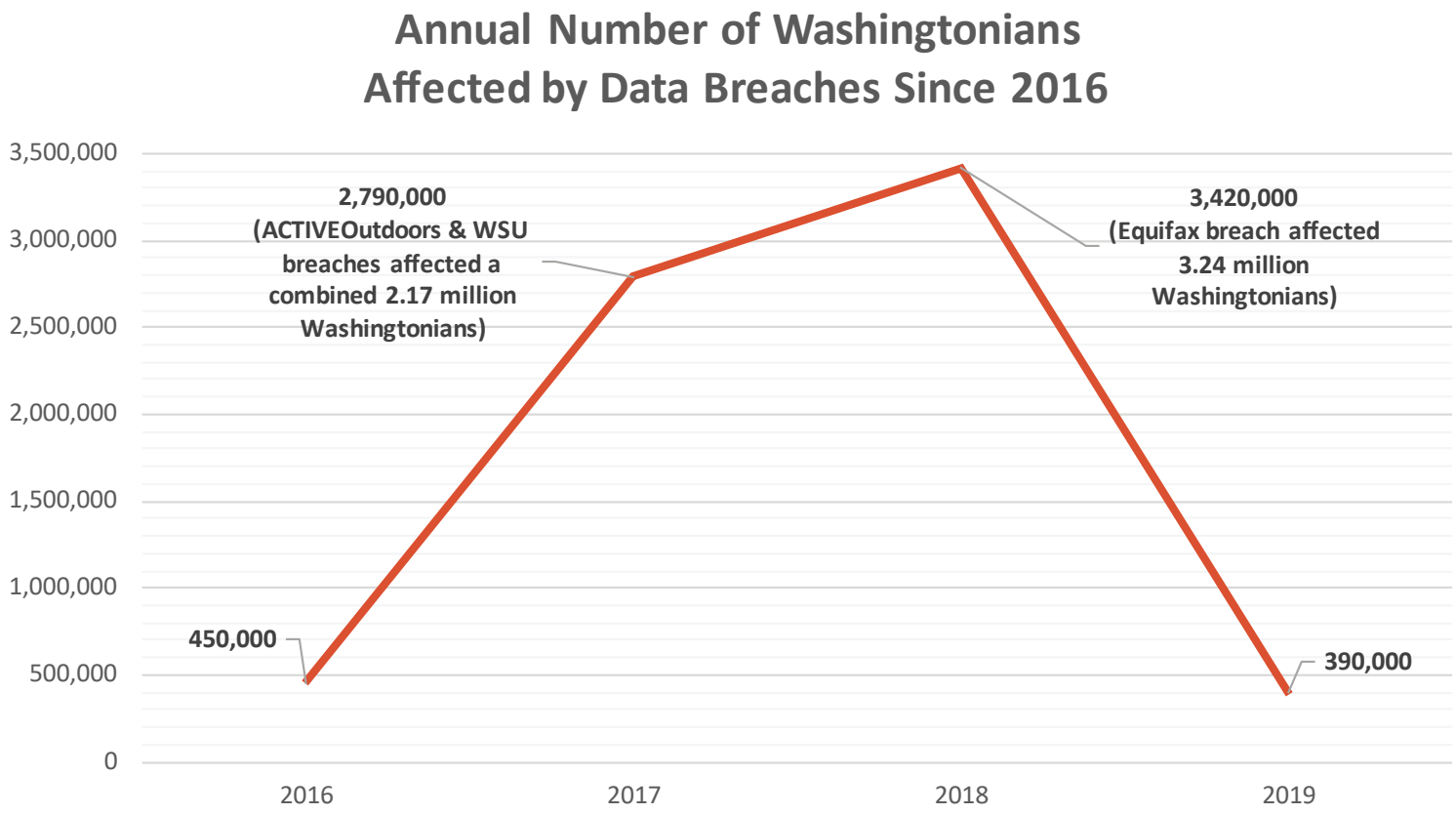
For the remaining 28, half of these cyberattacks were conducted with malware. This is particularly of concern because malware—and spyware specifically—can be very challenging to detect and often lead to breaches that can go undetected for a significant amount of time.

The large volume of malware attacks relative to other types of cyberattacks may also be indicative of a trend on the part of cyber criminals toward relying on more covert and sophisticated methods of breaching data.

A skimmer being installed on an ATM.

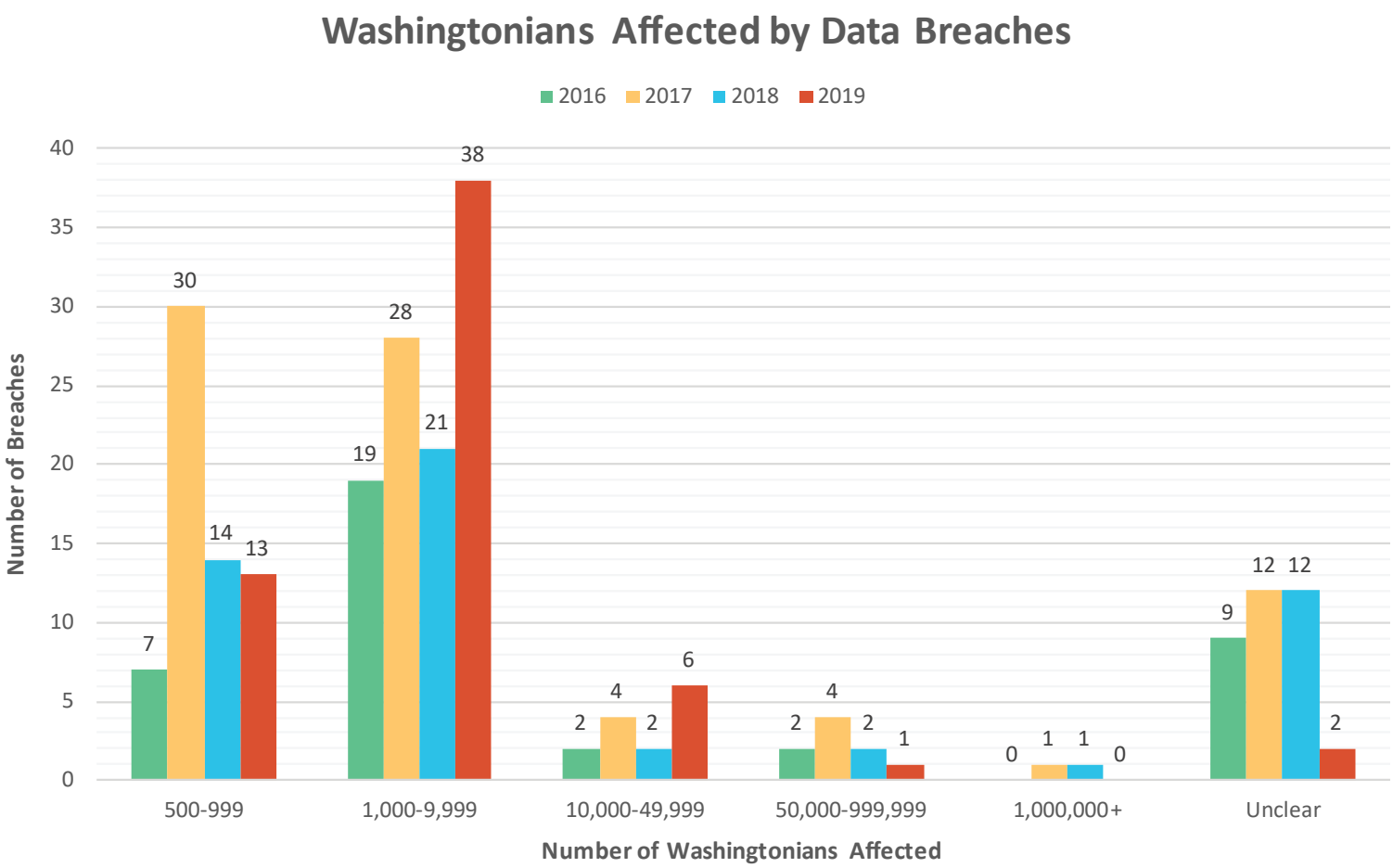
Source: Washington State Department of Financial Institutions

Number of Washingtonians Affected



In 2019, 60 data breaches affecting more than 500 Washingtonians' personal information were reported to the Attorney General's Office. This is up from 2018's 51 reported breaches. Although the total number of breaches increased, the total number of Washingtonians affected by these breaches is significantly lower, from 3.4 million in 2018 to approximately 390,000 in 2019.

This decrease is attributable to the fact that our office was only notified of one breach affecting 50,000 or more Washingtonians in 2019, compared to five in 2017, and three in 2018, including the Equifax mega breach which alone affected 3.2 million Washingtonians.



By a significant margin, the majority of data breaches reported to our office in 2019 compromised the personal information of between 1,000 and 9,999 Washington residents. This is the second straight year that a majority of breaches have affected at least 1,000 Washingtonians. 2019 also marks the highest number of breaches affecting between 1,000 – 9,999 Washington residents since our office started tracking this data, increasing from 21 breaches in 2018, to 38 this year.

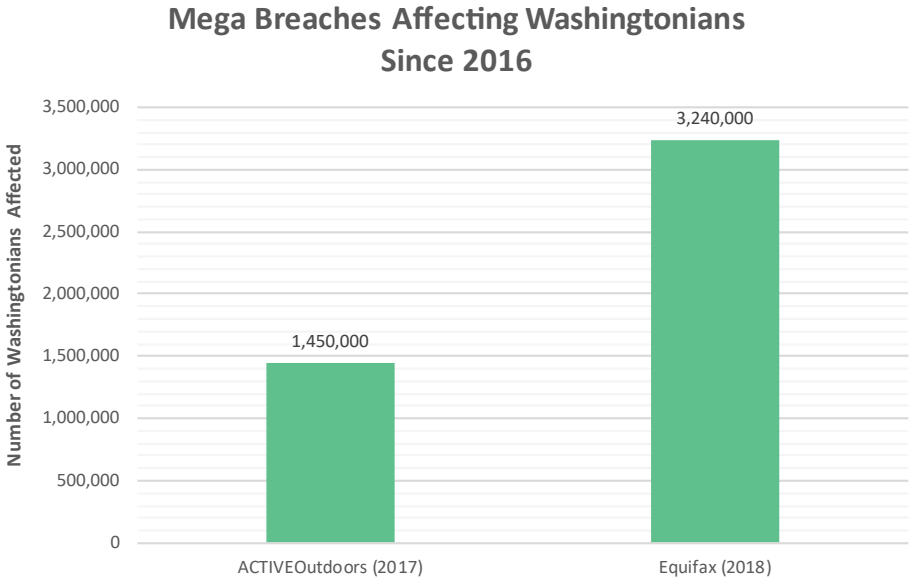
What are "Mega Breaches"?

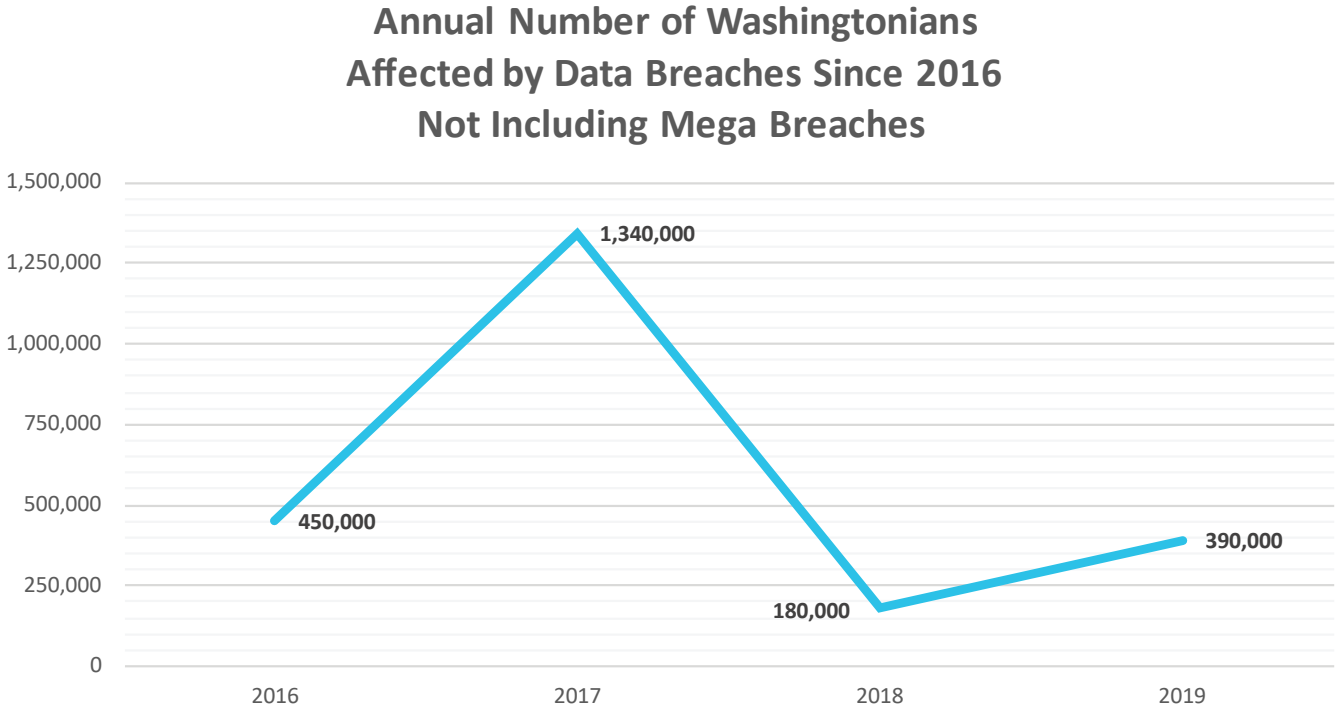
For the purposes of this report, a mega breach is any breach that affects the personal information of 1 million or more Washington residents. These breaches have a tremendous impact on the total number of Washingtonians impacted by data breaches each year, often impacting more people in a single breach 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. Looking ahead to next year, Capital One announced a potential mega breach on July 29, 2019 affecting an estimated 100 million individuals in the U.S., although we do not yet know how many Washingtonians were impacted.[1]

Number of Washingtonians Affected

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 2019 "Cost of a Data Breach Report," (Ponemon Report) breaches compromising 1 million or more records cost an estimated $42 million per breach, and breaches affecting more than 50 million records cost an estimated $388 million.[2]



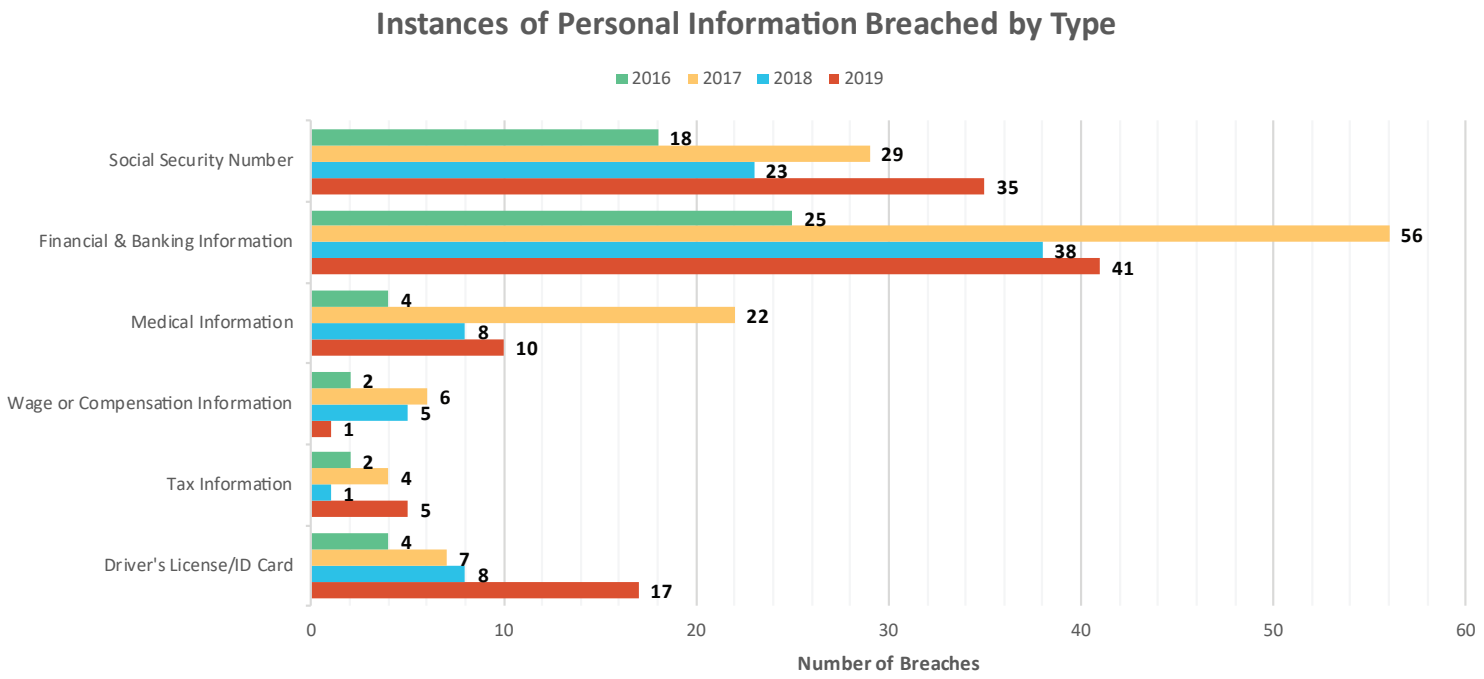


Due to their massive size, mega breaches also obscure trend data for the much more common small to mid-size breaches.

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 nearly doubled from 2018, caused by the significant increase in small to mid-size breaches affecting Washingtonians this year.

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.

Types of Personal Information Compromised



Note: This chart does not include every category of PII that was reported to our office in 2019. In subsequent reports, additional categories will be included and tracked to reflect changes made to Washington's definition of PII in RCW 19.255.010 and RCW 42.56.590.

Washington law requires notification to the Attorney General's Office when a data breach includes personally identifiable information (PII). Under the current definition of PII in Washington State, this data includes an individual's first name or first initial and last name in combination with any of the following:[3]

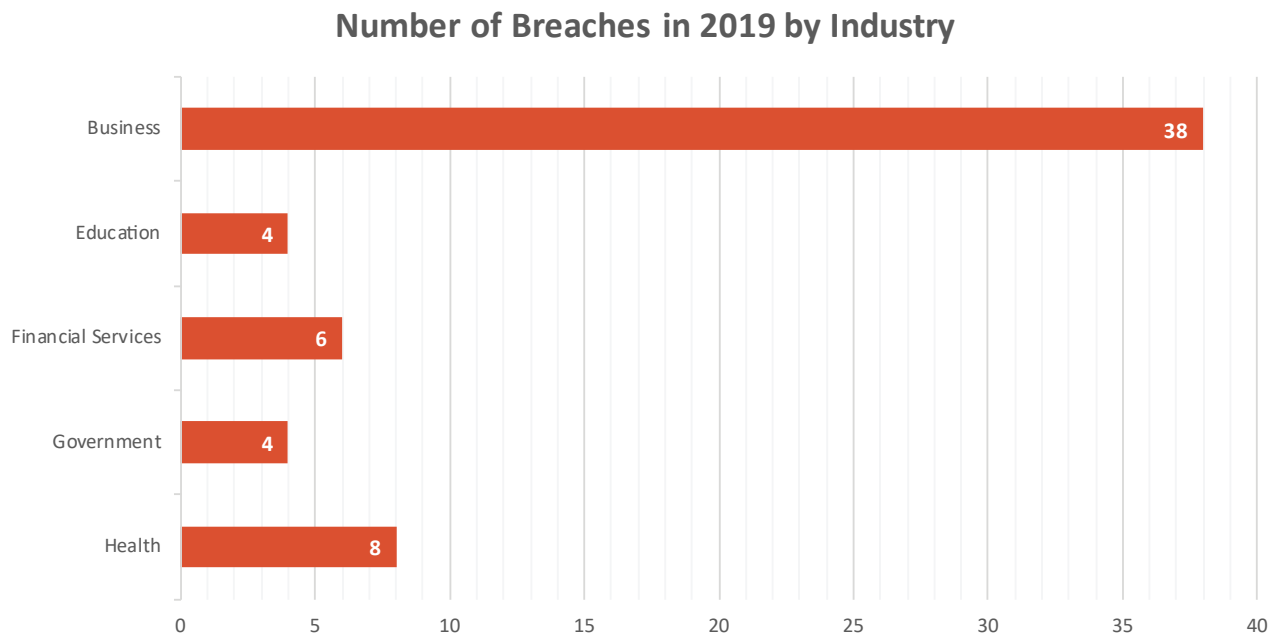
- Social Security number (SSN);
- Driver's license or Washington identification card number; or
- Financial account numbers, including payment card information, in combination with a security or access code, or password that would allow access to the financial account.

For the fourth straight year, financial information was the most commonly compromised type of personal information.

41 breaches, representing more than two-thirds 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).

Also of note, the number of breaches targeting SSNs rose by nearly 50%, from 23 breaches in 2018 to 35 in 2019. This is nearly tied with the number of breaches compromising financial data in 2019, and sets a new record for total number of breaches affecting SSNs since the Attorney General's Office began publishing this report in 2016.

Industries Reporting Breaches

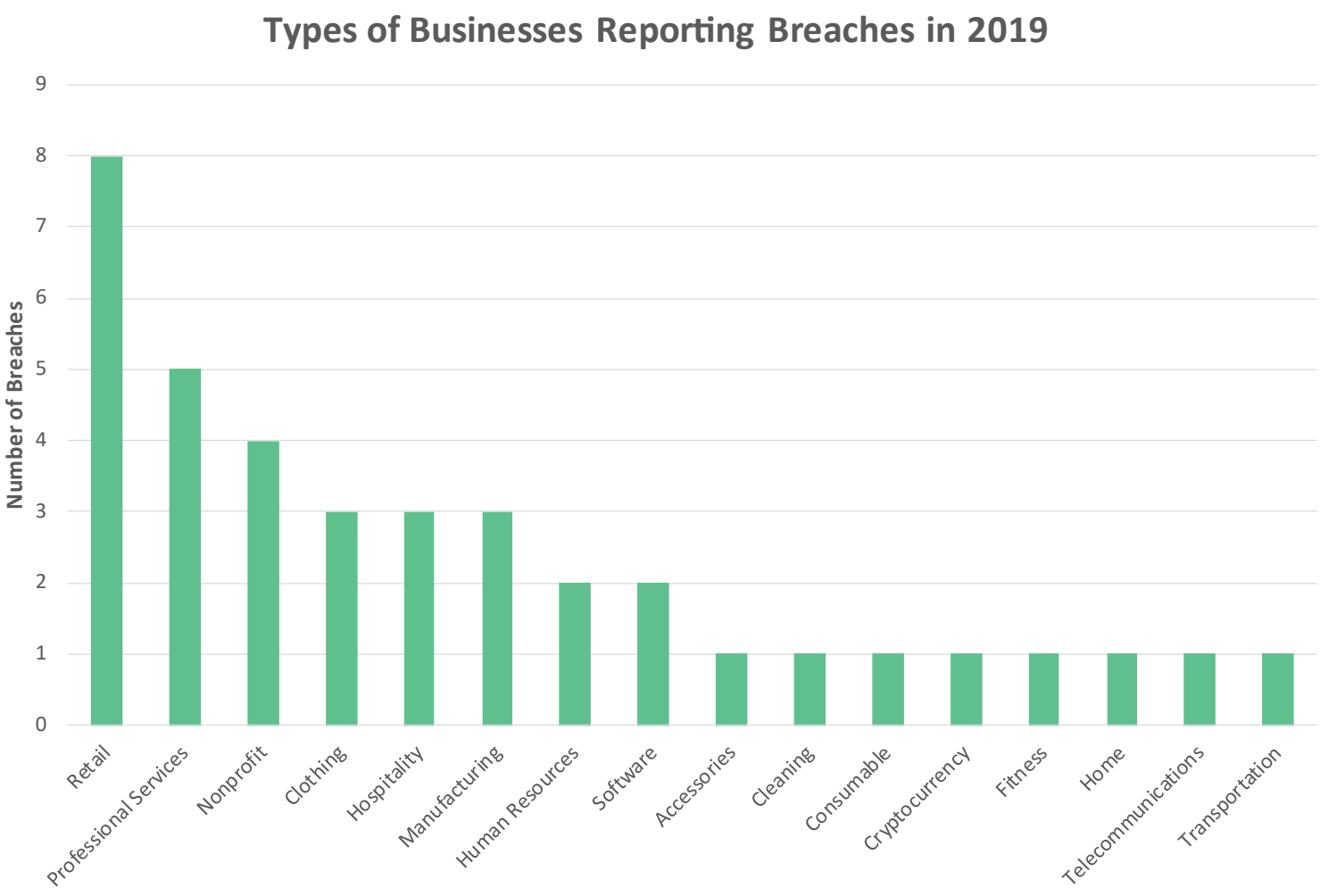


The Attorney General's Office also tracks breaches by industry. Consistent with earlier reports, our office uses industry categories based on the Identity Theft Resource Center's classifications, including:

- Business;
- Education;
- Financial services;
- Government; and
- Healthcare.

The business category includes 23 sub-categories, including retail, nonprofit, transportation, human resources, hospitality, manufacturing, and software.

Continuing the trend from the last two years, the majority of breaches reported in 2019 came from organizations categorized as businesses, which accounted for over 60% of all breaches. Malicious cyberattacks were responsible for nearly 80% of these data breaches, most commonly through phishing e-mails and malicious code installed onto servers or websites.



Within the business category, the Retail (21.1%), Professional Services (13.2%), and Nonprofit (10.5%) sub-categories were the most common types of businesses to be breached, representing nearly half of all breaches reported to our office by businesses in 2019.

Although businesses were the most frequently breached industry in 2019, the Health industry had the largest number of affected Washingtonians. Breaches of businesses in 2019 affected on average 3,831 Washingtonians per breach, and accounted for approximately 35% of all Washingtonians impacted by data breaches in 2019. This was second only to the Health industry, which saw an average of 27,041 Washingtonians affected per breach, representing 55% of all Washingtonians impacted in 2019. This is largely due to the January 2019 ransomware attack at Columbia Surgical Specialists, which affected aproximately 130,000 Washingtonians.

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 to an American business in 2019 is $242 per compromised record, up 3.8% from 2018.[4] The study found that, of the $242 per compromised record, $154 relates to indirect costs (such as turnover of customers resulting from the breach) and $88 comes directly from the breach (including legal fees, credit monitoring services for consumers, and security improvements).

The study also found that, globally, malicious attacks remain the primary cause of data breaches – approximately 51% of the cases studied in 2019 – and are still the most expensive type of data breach for businesses. The large spike in cyberattacks that were reported to our office this year reflects this global trend, and is an indication that data breaches continue to be a major threat to Washington businesses and their consumers.

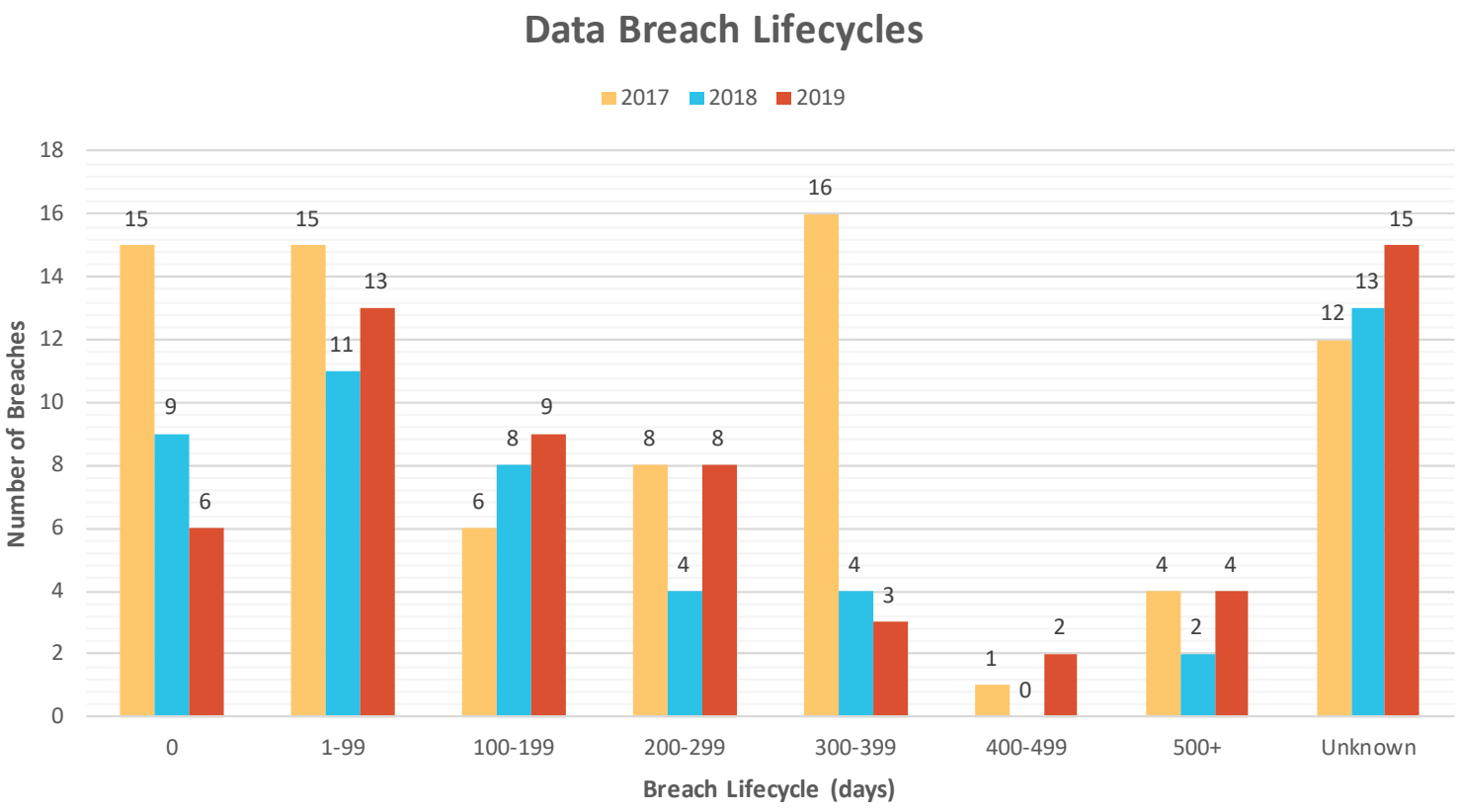
It also underscores the importance of businesses planning for and being prepared to address a breach of their records.

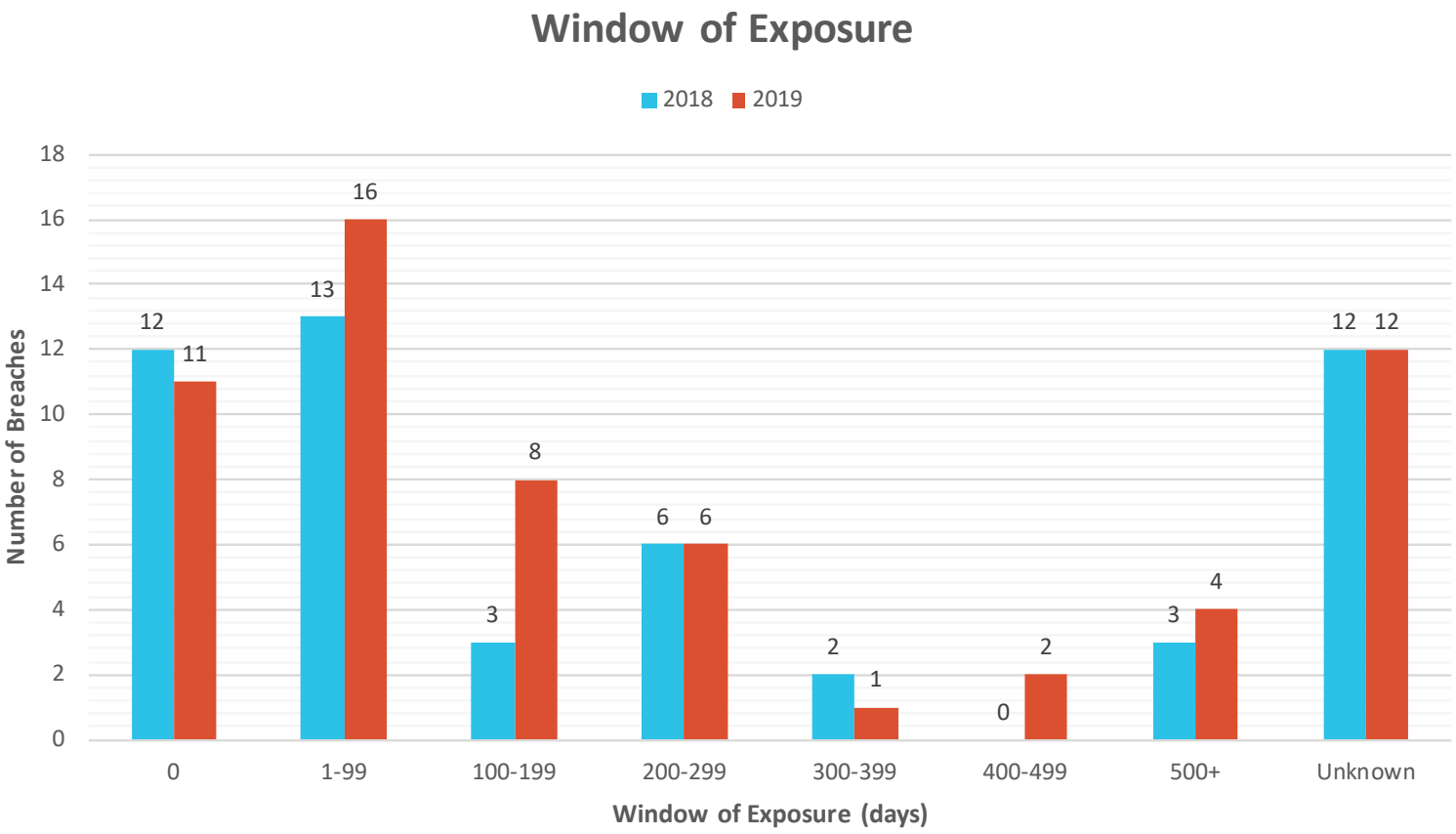
The Ponemon Report notes that businesses that had an incident response team and extensive testing of their response plans prior to a breach saved an average of over $1.2 million per incident in 2019.

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 represented as the sum of these two measurements. This is referred to as the "lifecycle" of a breach.



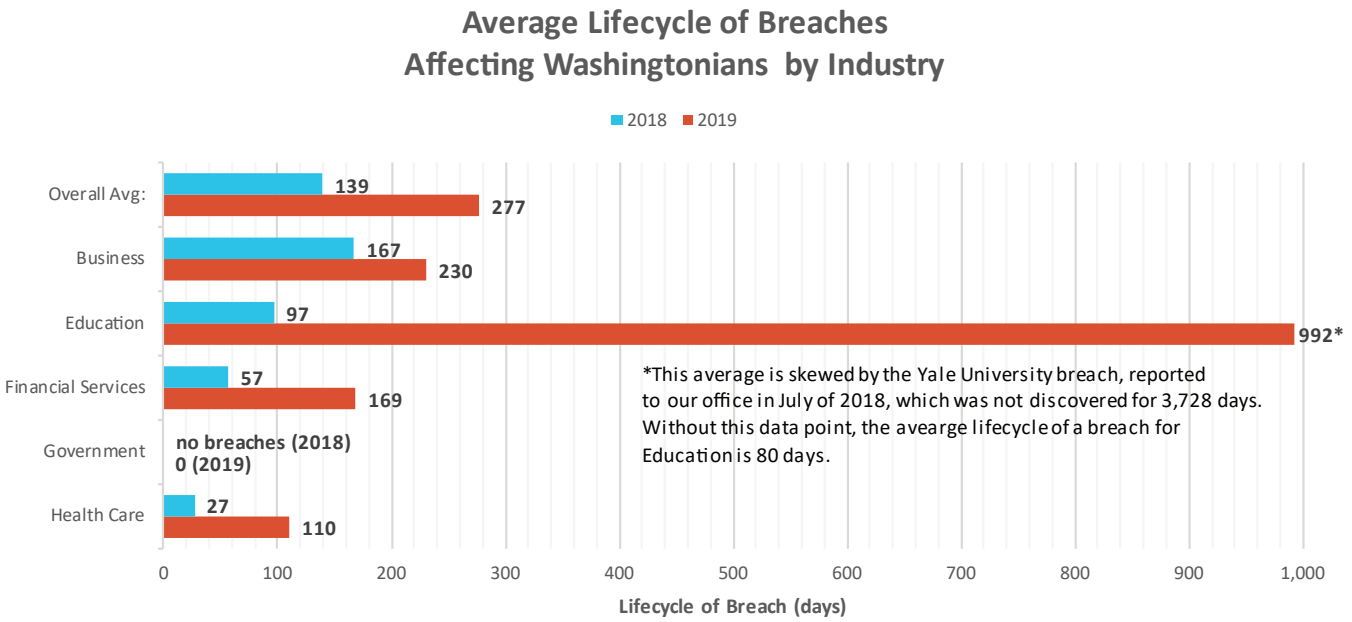


This is not to be confused with the period of time in which a breach is active, also known as the "window of exposure." The ongoing theft of information often concludes before it is discovered by the breached entity. This was the case in 28 (58%) of the breaches reported to the Attorney General's Office in 2019. 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 clear example of this can be found in a breach that occurred at Yale University, and was reported to our office in July of 2018. In this case, intruders gained access to a Yale database for nearly a full year, between April 2008 and January 2009. This represents a window of exposure of approximately 275 days. However, officials at Yale did not discover that the breach had occurred until June 2018 when they conducted a security review of Yale's servers – almost a decade after the breach's conclusion. As a result, the lifecycle of this breach was significantly longer than the window of exposure. 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 2019 had a window of exposure of less than 200 days, and a lifecycle of less than 300 days. On average, breaches with a lifecycle of less than 300 days in 2019 affected approximately 6,000 Washingtonians each.

There were also a significant number of breaches in 2019 where the window of exposure or lifecycle could not be determined from the notification provided to our office, categorized as "Unknown." For data on lifecycles, this represents the single largest category of such data with 15 cases in 2019 affecting an average of 12,549 Washingtonians per breach.



The Average Lifecycle of Breaches by Industry

The average lifecycle of a breach increased significantly for all industries in 2019. On average, breaches reported to the Attorney General's Office had a lifecycle of 277 days, a 99% increase from 2018 when the average was 139 days.

The significant increase in lifecycle length in 2019 is 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.

It is possible that 2019 will prove to be an outlier. There were two breaches in particular that significantly impacted this data, including the breach at Yale, which took over 3,000 days to discover. However, even without these two potential outliers, the average time to discover a breach remains significantly higher than 2018, at 192 days – a 42% increase.

2019's lifecycle data could be an indication of the growing challenge of detecting breaches as cyber criminals increasingly rely on more complex and covert methods of breaching security systems using malware.

How Long Did Businesses Take to Resolve Breaches?

Excluding the Yale University breach, the average lifecycle of a breach was longer for businesses than any other industry, with an average of 230 days per breach. This represents a 38% increase for businesses since 2018's report, when the average was 167 days. Of the 38 businesses reporting data breaches to the Attorney General's Office in 2019, 32 specified the amount of time it took them to identify the data breach. Of those 32, less than half reported that they had discovered the data breach fewer than 100 days after it began. 13 businesses (41%) reported a breach 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, $1.2 million per breach compared to their counterparts who took more than 200 days.[5] Notably, the 2019 Ponemon Report also states that the global average lifecycle of a breach across all industries is 279 days. For breaches reported to our office, the 2019 average was 277 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 must be provided without unreasonable delay, no more than 45 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.

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:

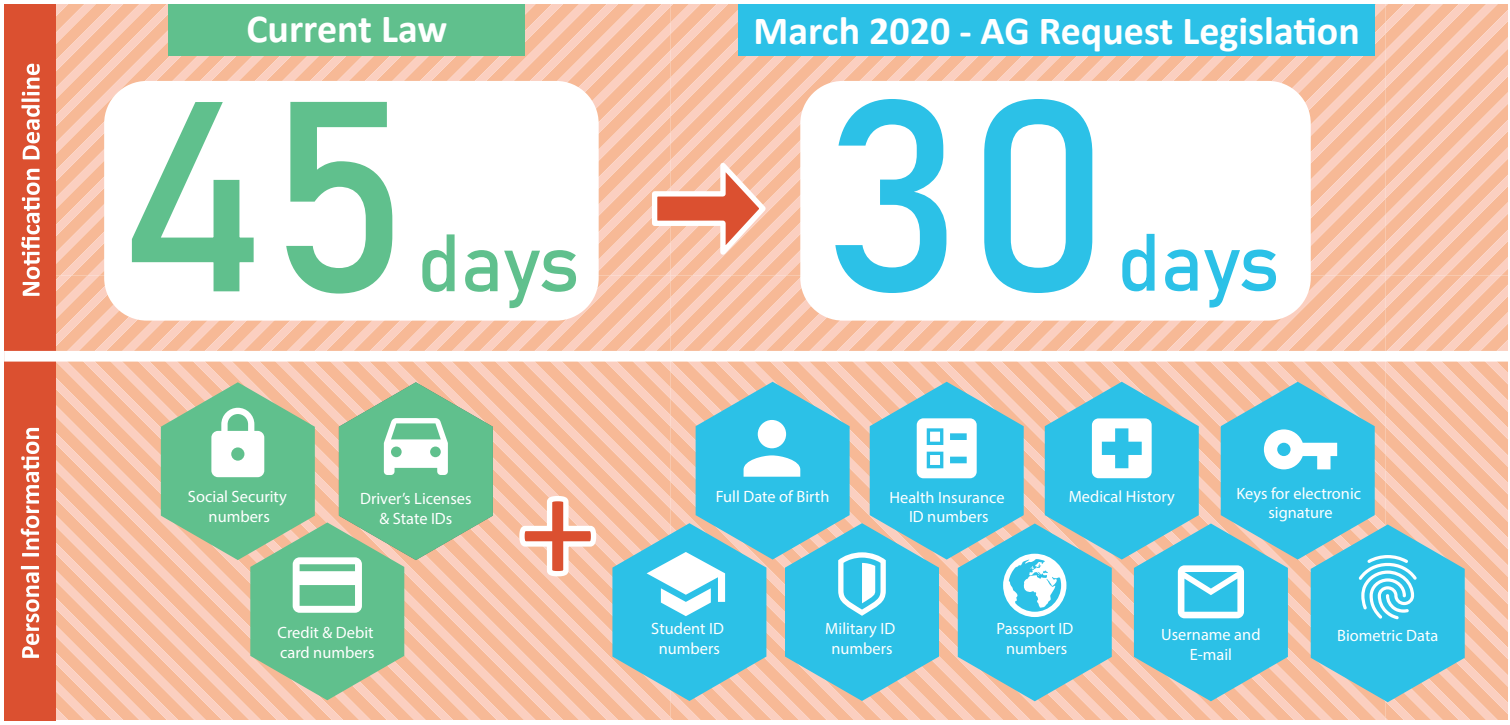
- Social Security number;
- Driver's license number or Washington identification card number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to their account.

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.

Strengthening Washington's Data Breach Law



Attorney General Ferguson requested legislation during the 2019 legislative session to improve our state's data breach law in the wake of the concerning trends highlighted in previous reports. Rep. Shelley Kloba (1st District) and Sen. Joe Nguyen (34th District) sponsored companion bills in the House and Senate. HB 1071 unanimously passed both chambers. On May 7, Gov. Inslee signed the bill into law. It goes into effect on March 1, 2020.

Gov. Inslee signing HB 1071 into law on May 7, 2019.

Rep. Shelley Kloba
(1st District)

Sen. Joe Nguyen
(34th District)

The updated law will enhance consumer data breach notification requirements by expanding the definition of "personal information" to include:

1. First name or initial and last name in combination with one or more of the following:
   a. Full date of birth;
   b. Private keys for electronic signature;
   c. Student, military, or passport identification numbers;
   d. Health insurance policy or identification numbers;
   e. Medical information, including medical history, mental or physical condition, diagnoses, or treatment; and
   f. Biometric data;

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

3. Username or email address in combination with a password or security questions and answers that would permit access to an online account.

The updated law also requires breached entities to provide the period of exposure in their notice to consumers, including the date of the breach and its discovery, and must provide the notice no later than 30 days after the breach was discovered.

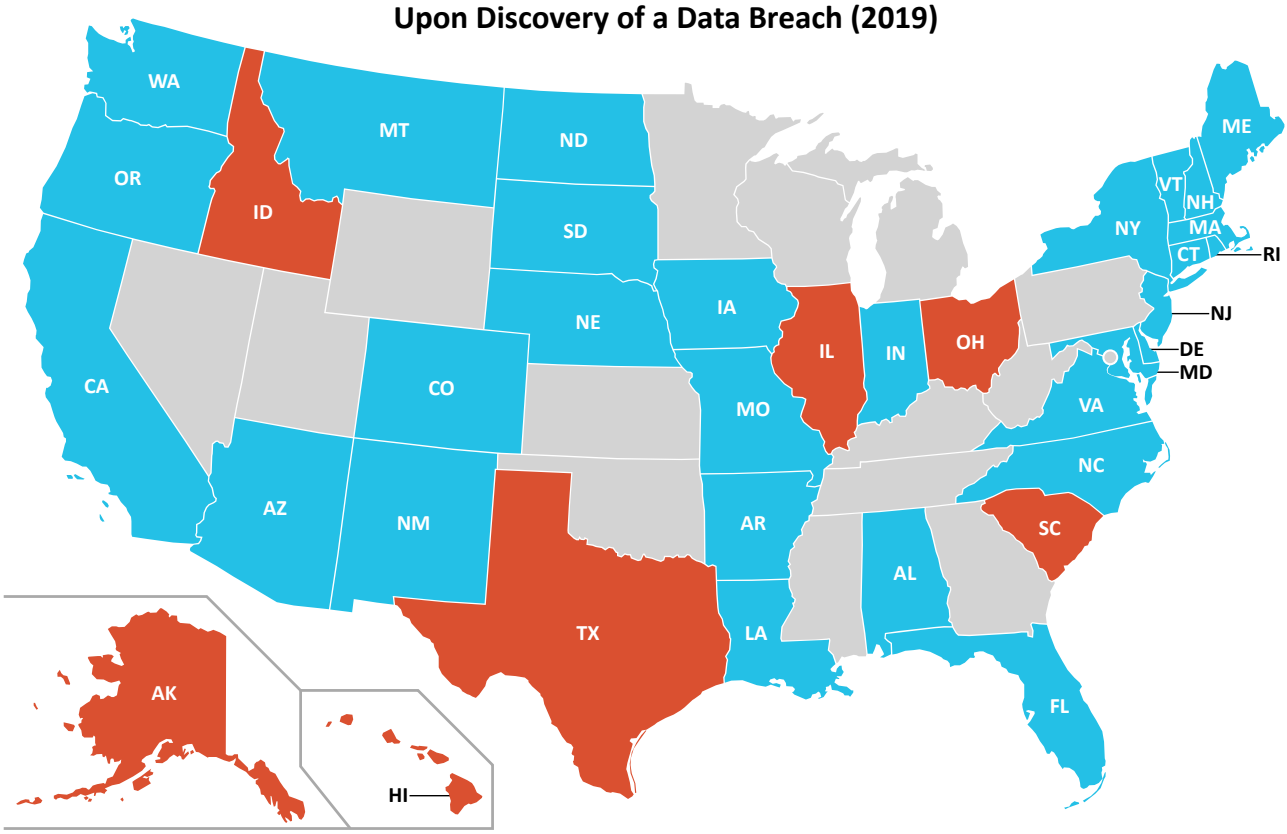
Likewise, notice must be provided no later than 30 days after discovery to the Attorney General's Office for any breach affecting more than 500 Washingtonians, and must include:

- 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.

How Does Washington's Law Compare to Other States?

States Requiring Notification of State Attorney General Upon Discovery of a Data Breach (2019)

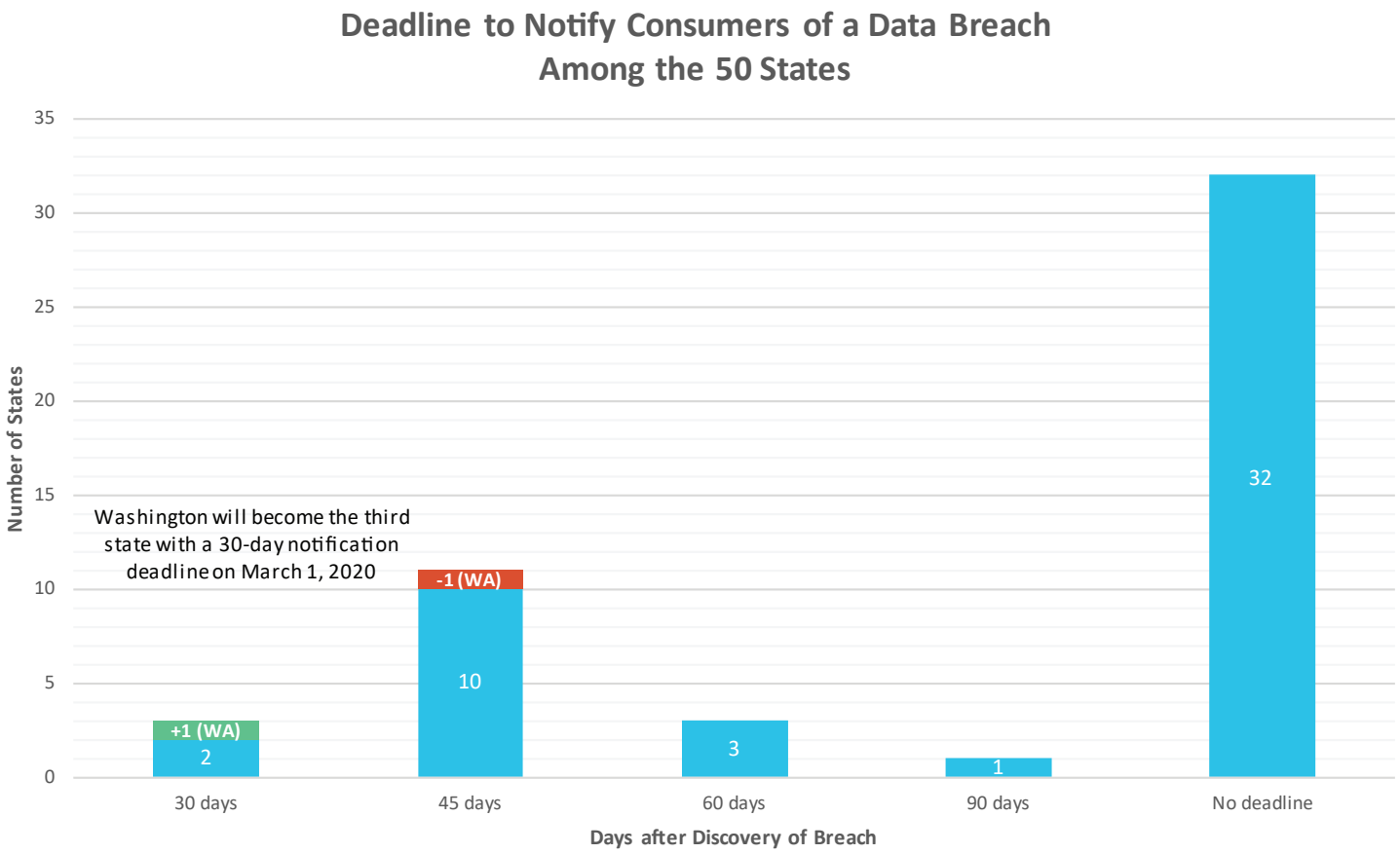


*States in **orange** only require notification to the Attorney General under special circumstances (e.g. Idaho & Illinois only require notice from public agencies), and/or require notification to a state agency that is not the Attorney General (e.g. Hawaii requires notice to the Office of Consumer Protection).

Washington Compared to Other States

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

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 personally identifiable information readable or usable has been breached together with the encrypted information.

In 36 states, including Washington, entities experiencing a breach must notify the Attorney General or another state agency. 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. In Illinois, state agencies need only report a breach to the Attorney General if it affects more than 250 Illinois residents, and need only do so within 45 days of discovering the breach. Unlike Washington, neither state has an explicit deadline to notify consumers for breaches affecting private entities.

In fact, only 18 states, including Washington, have a specific deadline for reporting breaches to consumers. As of August 2019, 12 states, including Washington, have a 45-day deadline to notify consumers. Florida and Colorado have the shortest deadline, 30 days.

Washington will become the third state with a 30-day deadline when our state's updated law goes into effect in March 2020. Most states with a deadline, including Washington (RCW 19.255.010 (16)), are triggered upon the discovery of a breach of personally identifiable 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."

Defining Personally Identifiable Information

All 50 states have the same general definition of personally identifiable information (PII):

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;

How Does Washington's Law Compare to Other States?

Data Element	States With That Element in Their Definition of PII
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, Colorado, Florida, Maryland, ***Washington***, Wyoming
Passport ID number	Alabama, Arizona, Colorado, Delaware, Florida, Louisiana, Maryland, North Carolina, Oregon, ***Washington***
Individual taxpayer ID number	Alabama, Arizona, Delaware, Maryland, Montana, North Carolina, Virginia, Wyoming
Tribal ID number	Rhode Island, Wyoming
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, Virginia, ***Washington***, Wyoming
Biometric data	Arizona, Arkansas, Colorado, Delaware, Illinois, Iowa, Louisiana, Maryland, Nebraska, New Mexico, North Carolina, Oregon, South Dakota, Wisconsin, ***Washington***, Wyoming
DNA profile	Delaware, Wisconsin
Username and password	Alabama, Arizona, California, Colorado, Delaware, Florida, Illinois, Maryland, Nebraska, Nevada, South Dakota, ***Washington***, Wyoming
E-mail address and password	Alabama, Arizona, California, Colorado, Delaware, Florida, Illinois, Maryland, Nebraska, Nevada, Rhode Island, South Dakota, ***Washington***, Wyoming

This table is representative of state laws around the country, effective Aug. 2019. It also includes Washington's updated law, effective March 2020.

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.

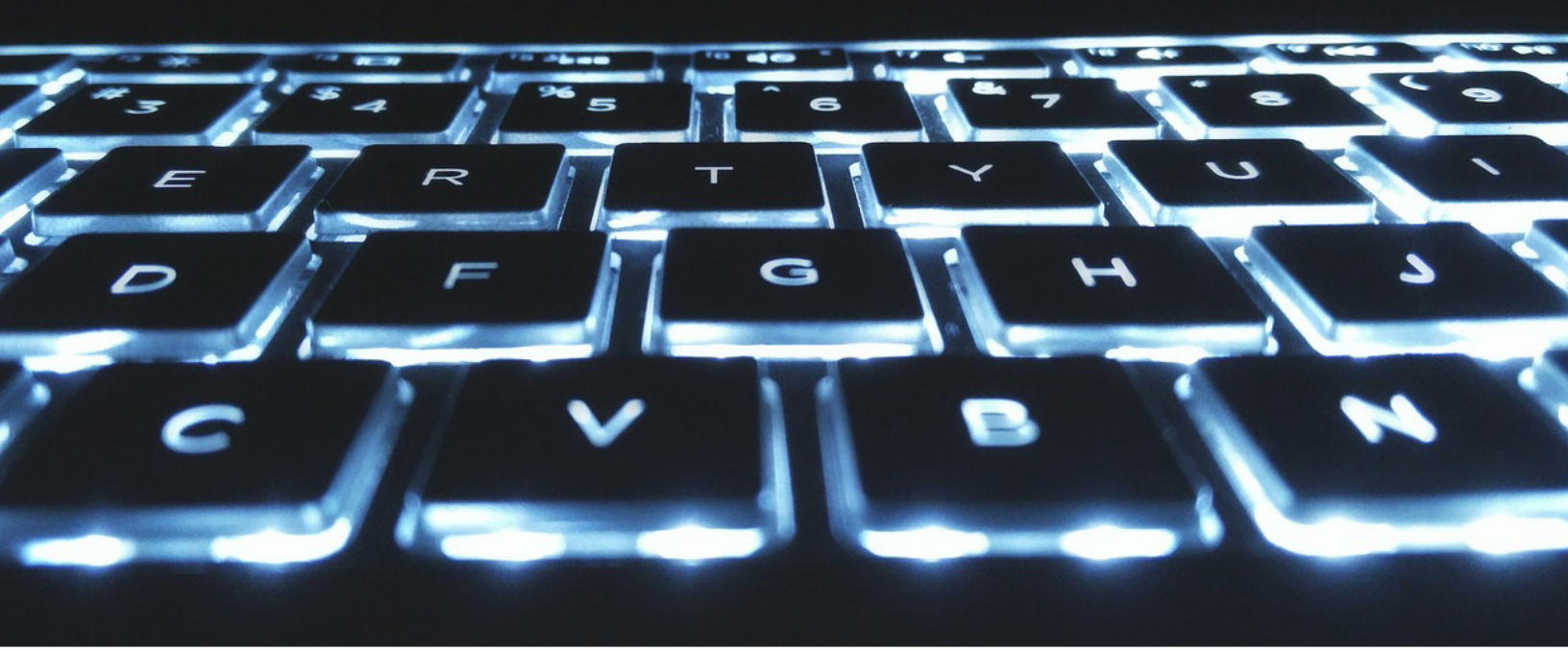
However, many states include additional data elements in their general definition of PII, including Washington beginning in March 2020. There are still a few elements included in various other states' laws that were not considered in the updated Washington law, including individual tax ID numbers, tribal ID numbers, birth or marriage certificates, DNA profile, and mother's maiden name.

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.[6]

Massachusetts' law, conversely, requires names to be part of the breach of financial information to trigger notice, but not passwords or security codes.[7] 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.[8]

For a detailed breakdown of Washington's current notification statute see: **Washington's Data Breach & Data Security Laws** (p.20), and for updates to the law coming in 2020 see: **Updates to Washington's Data Breach Law** (p.21).



Conclusions & Recommendations

Data breaches continue to be a significant concern for Washingtonians in 2019 and beyond. Despite the overall number of affected consumers decreasing from 2018, the total number of breaches reported to our office and the average length of a breach's lifecycle increased this year. These trends highlight the importance of the data breach legislation passed in the most recent session, which will require earlier and more detailed notice to consumers of a breach for a greater variety of their data, giving Washington 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. **Expand the definition of "personal information" in RCW 19.255 and RCW 42.56 to include Individual Tax Identification numbers (ITINs) and Tribal ID numbers.**

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, eight states include ITINs in their definition of "personal information." Policymakers should give strong consideration to making Washington state the ninth.

Tribal ID cards are issued by tribes as proof of enrollment and membership in the tribe and in certain cases can be used in lieu of a state or federally issued ID card. Typically, these cards include an enrollment number that, if stolen, could be used for the purposes of identity theft, and thus are of a similar sensitivity to state-issued ID card numbers. As such, policymakers should consider adding them to the definition of "personal information" under our state's data breach notification statutes. At present, both Rhode Island and Wyoming include Tribal ID numbers in their state's definition of "personal information."[9, 10]

2. **Amend the definition of "personal information" in RCW 19.255 and RCW 42.56 such that breaches of Financial Information and Social Security numbers (SSNs) are standalone triggers for notice.**

Under Washington's data breach notification law, notice of the breach of either financial information or SSNs is only required if it is in combination with the associated individual's first name or initial and last name. While the breach of a full name in combination with either of these identifiers is particularly concerning, the rise of "synthetic identity theft" shows that the breach of either financial information or SSNs in isolation can be equally damaging.

Unlike traditional identity fraud, where a criminal assumes a real person's identity, synthetic identity fraud occurs when a criminal creates a new identity to commit financial crimes. This includes what the Federal Reserve calls "identity compilation," where a criminal combines fabricated information, like a fake name and date of birth, with real information, like a stolen SSN.[11]

According to the Federal Reserve's July 2019 report, "Synthetic Identity Fraud in the U.S. Payment System," these criminals often target the information of children, the elderly, or homeless individuals as they are the least likely to access their credit information and discover the fraud.[12] The report also estimates that synthetic identity theft is the fastest growing type of financial crime in the country, responsible for 20% of credit losses in 2016, and costing lenders around $6 billion that same year.[13]

As mentioned earlier, Washington would not be the only state to make the breach of these identifiers a stand-alone trigger for notification. In Colorado, financial account information does not need to be in combination with an individual's full name to trigger notice.[14] Likewise for SSNs in Indiana's data breach notification statute.[15]

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.**

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. According to the 2019 Ponemon Report, 48% of the companies surveyed lacked any form of security automation – security technologies used to detect breaches more efficiently than humans can.[16] For these companies, the average cost of a data breach was nearly twice as expensive as for those who implemented security automation.[17] Similarly, the formation of a dedicated Incident Response Team and testing of an Incident Response Plan on average reduced the total cost of a breach by more than $300,000.[18]

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.

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; and

4. File a report with your local police department.

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.

Basic steps businesses can take 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; and

3. Create and implement an information security plan.

Notes

1. "Information on the Capital One Cyber Incident," https://www.capitalone.com/facts2019, originally published July 29, 2019.
2. "2019 Cost of a Data Breach Report," Ponemon Institute, July 2019.
3. RCW 19.255.010, effective since July 2015.
4. "2019 Cost of a Data Breach Report," Ponemon Institute, July 2019.
5. Ibid.
6. Colo. Rev. Stat. Ann. § 6-1-716 (2006); as amended (2018).
7. Mass. Gen. Law Ann. Ch. 93H, §§ 1 (2007).
8. Ind. Code Ann. §§ 24-4.9 et seq. (2006); as amended (2009).
9. R.I. Gen. Laws §§ 11-49.3-2—49.3-6 (2015).
10. Wyo. Stat. Ann. §§ 40-12-501, 40-12-502 (2015).
11. "Synthetic Identity Fraud in the U.S. Payment System," United States Federal Reserve, July 2019.
12. Ibid.
13. Ibid.
14. Colo. Rev. Stat. Ann. § 6-1-716 (2006); as amended (2018).
15. Ind. Code Ann. §§ 24-4.9 et seq. (2006); as amended (2009).
16. "2019 Cost of a Data Breach Report," Ponemon Institute, July 2019.
17. Ibid.
18. Ibid.