Washington State
Attorney General's Office

2018
Data Breach Report

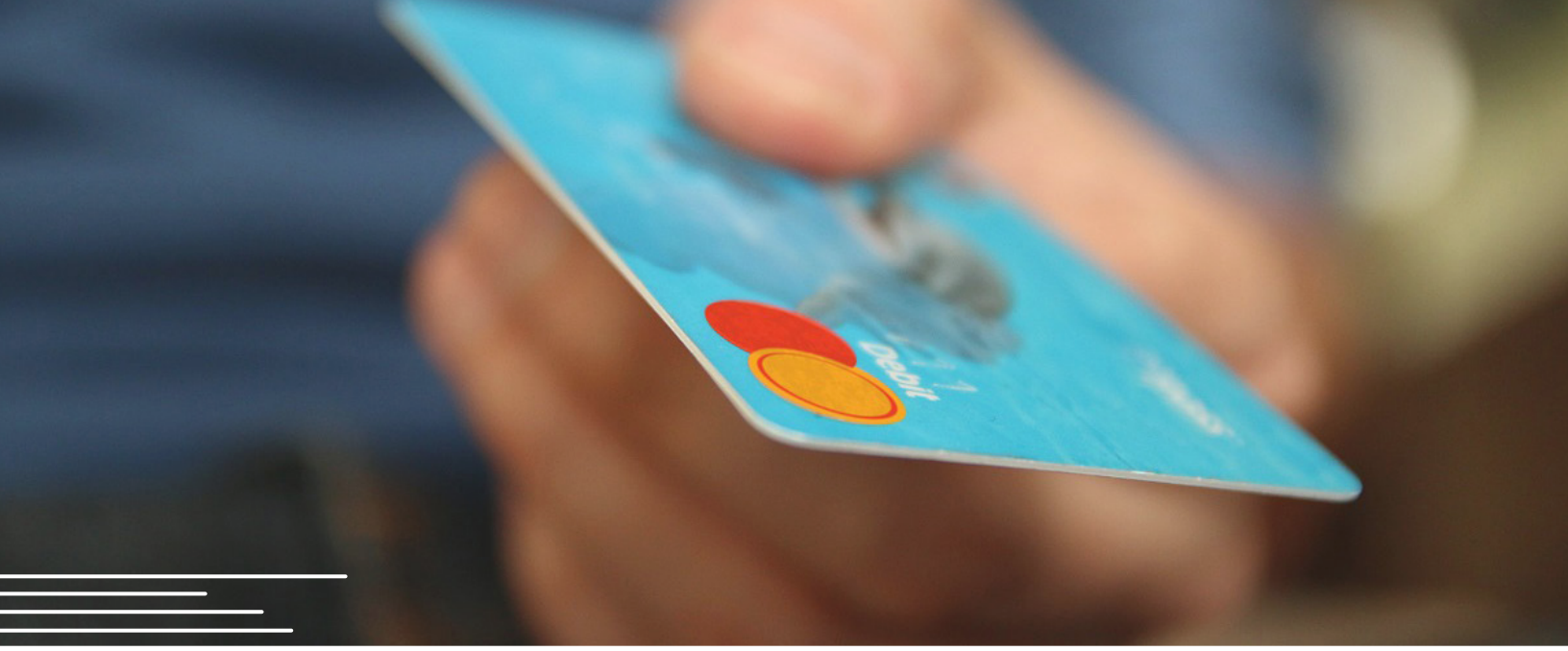


Table of Contents

Letter from Attorney General Bob Ferguson

October 2018

Dear Washingtonians,

Data breaches are a significant threat to Washington individuals and businesses. For the second straight year, the number of Washingtonians impacted by data breaches increased, with nearly 3.4 million Washingtonians affected in 2018. This represents a 26% increase compared to 2017 and more than 700% compared to 2016.

Given the trends reflected in this third annual edition of the Attorney General's Office Data Breach Report, it is critically important that organizations entrusted with sensitive data take steps to secure it. Policymakers should also consider taking further steps to strengthen our data breach notification laws so that Washingtonians can take appropriate steps when their personal information has been compromised.

During the past year, a diverse set of organizations experienced data breaches, including hotels, financial services, restaurants, and ride-share companies. Breaches befell these companies in a variety of ways. In one case, a company providing courier services to Timberland Bank discovered that bags containing loan files and paper checks had been stolen during transit between bank branches.

My office is taking action to protect Washingtonians when companies fail to reasonably secure data or fail to provide timely notice to impacted consumers. In November 2017, my office filed a multi-million-dollar consumer protection lawsuit against ride sharing company Uber for failing to disclose a data breach that compromised the names and driver's license numbers of nearly 13,000 Uber drivers in Washington. Uber was required to notify affected drivers and my office of the breach within 45 days, but instead Uber waited more than a year to provide the notice.

As a result of our lawsuit, Uber will pay $5.79 million for violating Washington state's data breach notification law, including $170 to most of the nearly 13,000 affected Uber drivers in Washington.

This report presents a summary of the data breach notices my office received over the past year. Tips and resources for individuals 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 security breach, or 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 businesses impacted by a data breach to notify Washingtonians whose personally identifiable information was compromised within 45 days of discovering the breach.

In 2015, Attorney General Ferguson proposed and the Legislature passed request legislation to strengthen Washington's data breach notification law. Among other changes, this legislation required notice to the Attorney General's Office when data breaches impact 500 or more Washingtonians.

This 2018 report covers data breach notifications received by the Attorney General's Office between July 24, 2017 and July 23, 2018. The data reveals:

- Malicious cyberattacks continue to be the leading cause of data breaches affecting Washingtonians.
- The total number of data breaches affecting Washingtonians decreased from 78 in 2017 to 51 in 2018. However, the total number of Washingtonians affected increased significantly, from 2.7 million in 2017 to 3.4 million in 2018.
- This sharp increase was a result of a single serious breach from one of the three major nationwide credit reporting agencies, Equifax, Inc. This breach compromised the personal information of an estimated 3.2 million Washingtonians.
- The majority of data breaches in 2018 affected between 1,000 and 9,999 Washingtonians – a shift from 2017 when the majority of data breaches affected less than 1,000 individuals.
- For the third straight year, financial information was the most commonly compromised type of data, reported in 38 of the 51 data breaches in 2018.
- In 2018, businesses on average took 167 days to identify and contain breaches. Less than half of businesses reporting breaches in 2018 discovered the breach within 100 days.

Recommendations

In light of these trends, our office recommends that policymakers reduce the deadline for notifying affected individuals and the Attorney General's Office to 30 days after discovery of a breach, including notification of the timeline of any individual data breach. Additionally, policymakers should expand the law to include a preliminary notification deadline to the Attorney General's Office within ten days, allowing our office to inform the general public of breaches sooner through Consumer Notices. Policymakers should also expand the legal definition of personally identifiable information that triggers these notices.

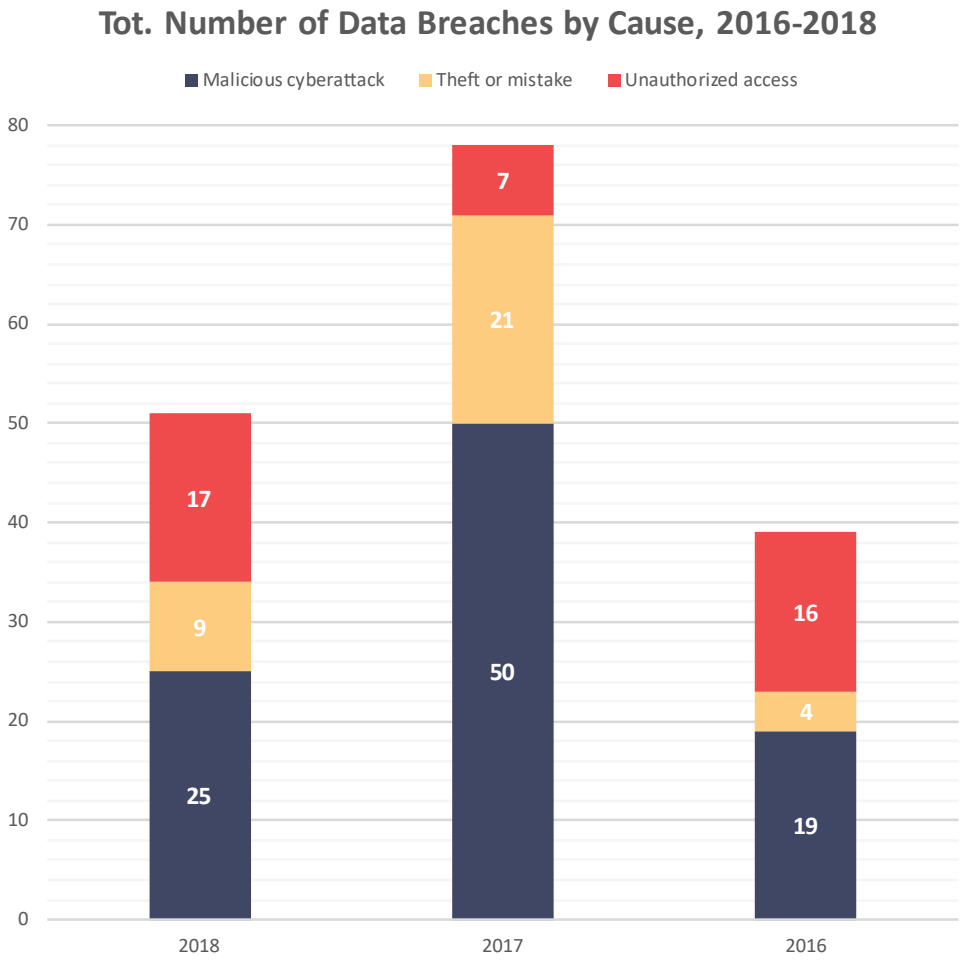
Causes of Data Breaches

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

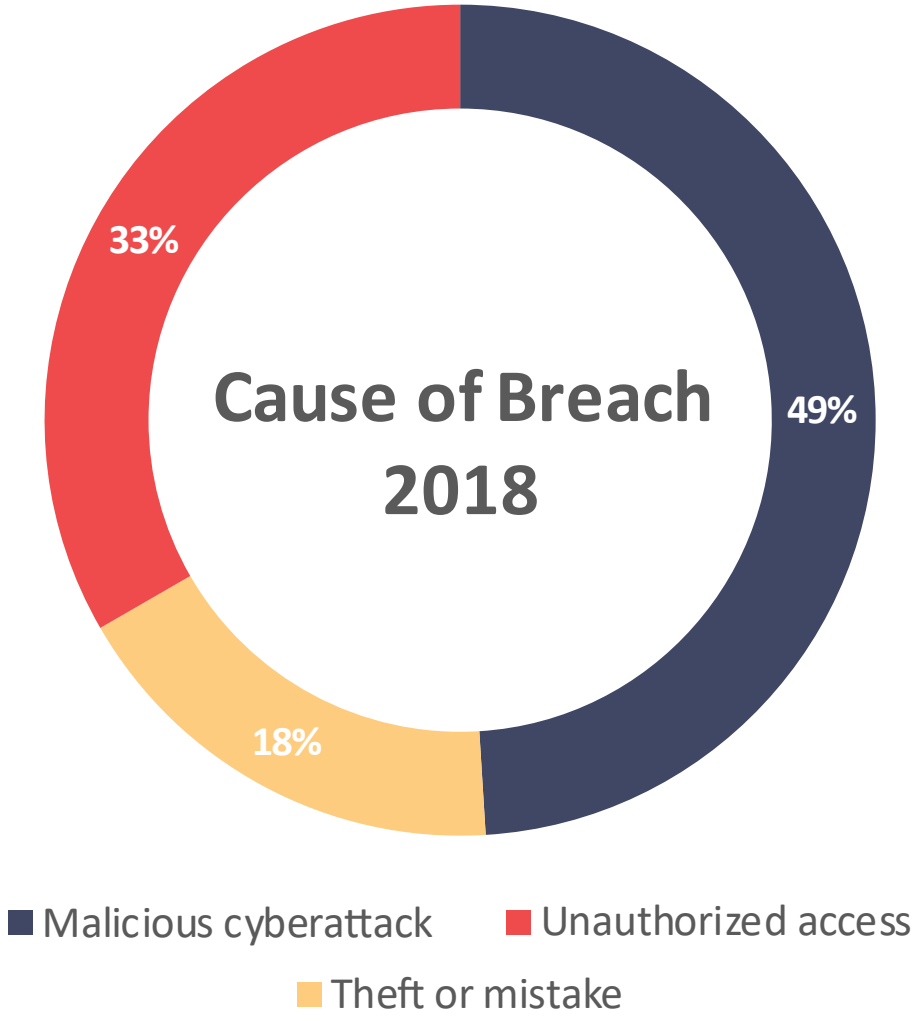
1. *Malicious cyberattack*: A third party deliberately attempts to gain or succeeds in gaining access to secure data stored on a server. The attack can use a virus, malware, phishing email, or similar means of accessing secure data remotely.

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 taking 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.



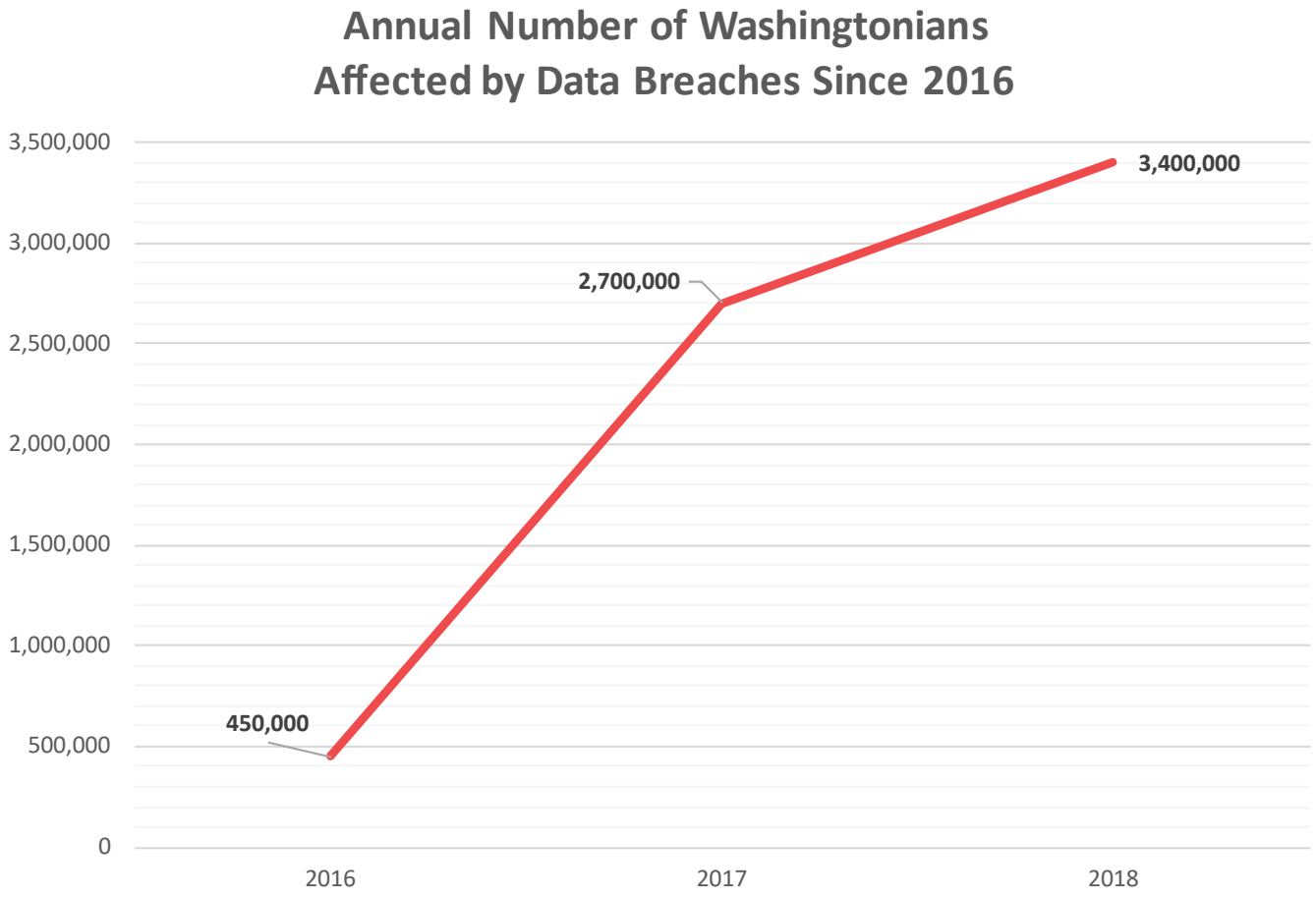
Causes of Data Breaches



Cause of Data Breach	Total 2018 Breaches	Percentage of 2018 Breaches	Total 2017 Breaches	Percentage of 2017 Breaches	Total 2016 Breaches	Percentage of 2016 Breaches
Malicious cyberattack	25	49.02%	50	64.10%	19	48.72%
Theft or mistake	9	17.65%	21	26.92%	4	10.26%
Unauthorized access	17	33.33%	7	8.97%	16	41.03%

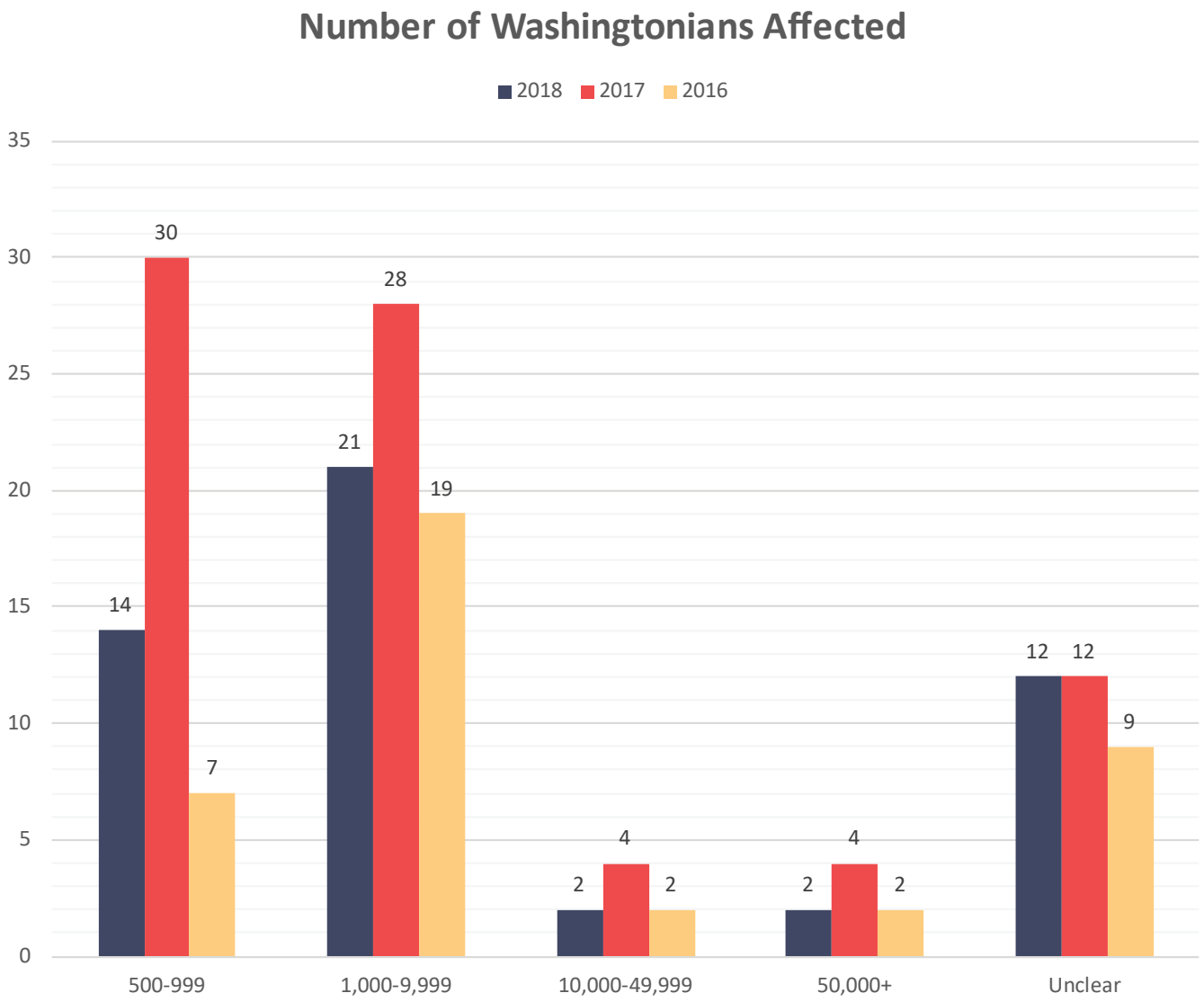
Nearly half of all data breaches affecting Washingtonians in 2018 were a result of cyberattacks. This is down from 2017, when nearly two-thirds of data breaches were caused by cyberattack. Of note, the percentage of breaches resulting from unauthorized access sharply increased in 2018, from 9% of breaches in 2017, to 33% in 2018.

Number of Washingtonians Affected



In 2018, 51 data breaches were reported to the Attorney General's Office that affected at least 500 or more Washingtonians' personally identifiable information. Despite a reduction in notifications to the Attorney General's Office from 2017, the total number of Washingtonians affected by these breaches increased by 26%, from 2.7 million in 2017 to 3.4 million in 2018.

Number of Washingtonians Affected



The preponderance of Washingtonians' data affected in 2018 came from a single massive data breach. The Equifax data breach, reported to our office on September 7, 2017, compromised the data of approximately 3.2 million Washingtonians. This data included Social Security numbers, names, dates of birth, addresses, driver's license numbers, and credit card numbers. This is more than double the number of Washingtonians affected by the ACTIVE Outdoors data breach (1.5 million), the largest individual data breach included in last year's report. The Equifax data breach alone is responsible for 95% of the Washingtonians affected by data breaches in 2018.

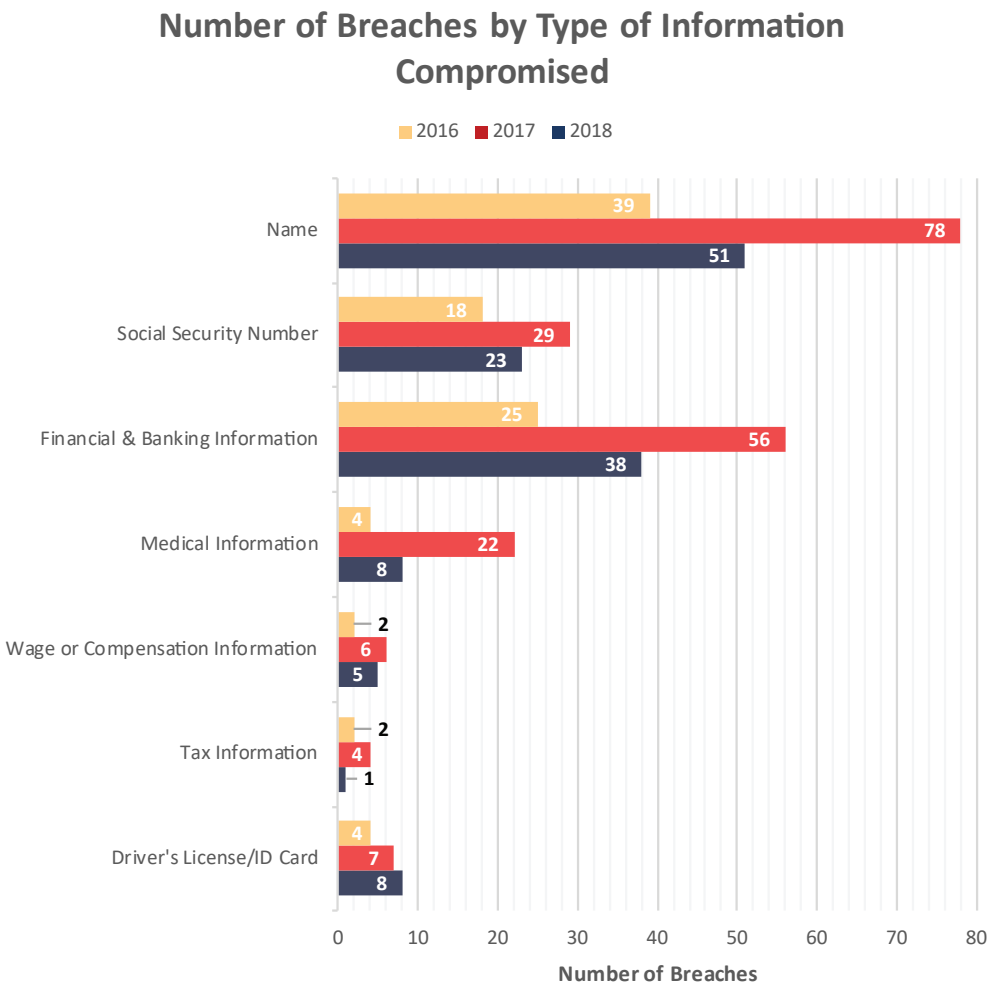
By a significant margin, the majority of the other data breaches in 2018 compromised the personal information of between 1,000 and 9,999 Washington residents. This represents a concerning shift from 2017, where the majority of data breaches reported affected less than 1,000 Washingtonians. This shift was a factor in the overall increase in the number of Washingtonians affected by data breaches in 2018.

Types of Personal Information Compromised

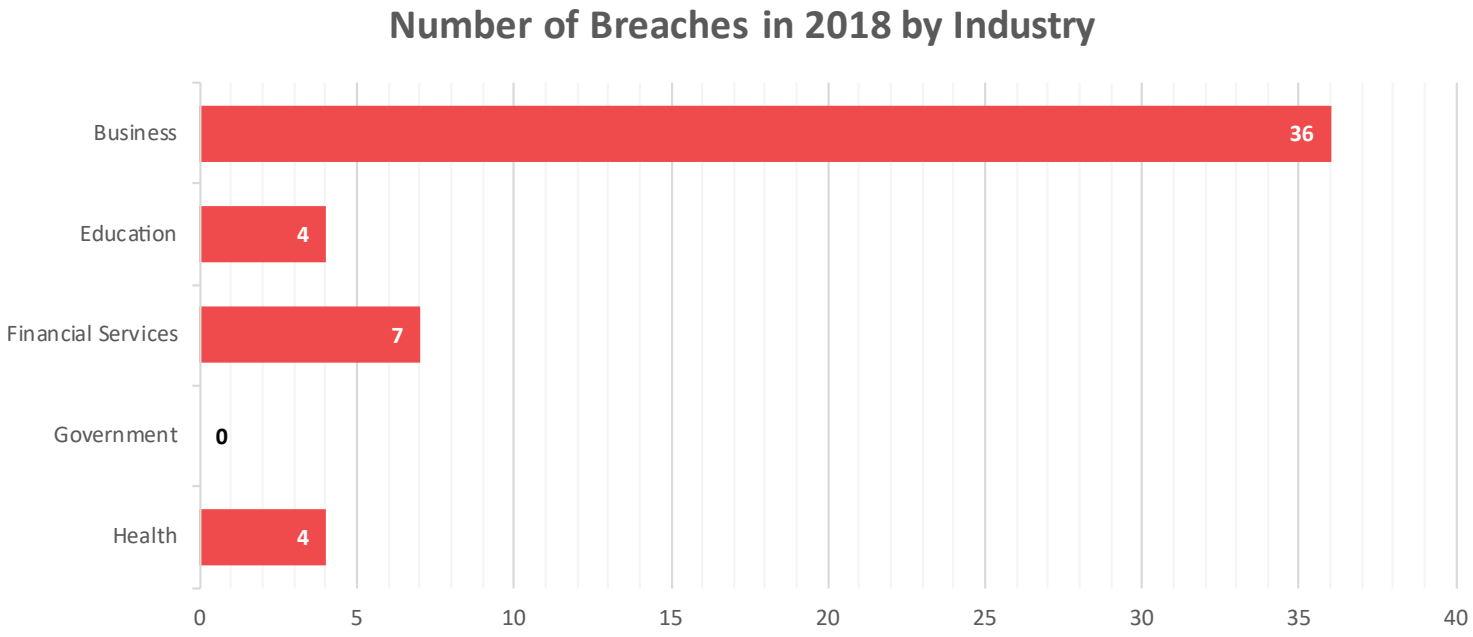
Washington law requires notification to the Attorney General's Office when a data breach includes someone's first name or first initial and last name in combination with any of the following:[1]

- Social Security number;
- Driver's license or 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 third year in a row, financial information was the most commonly compromised type of personal information. Three-quarters of all breaches reported this year resulted in the compromise of financial data. These 38 data breaches exposed more than three million individual financial records.



Industries Reporting Breaches



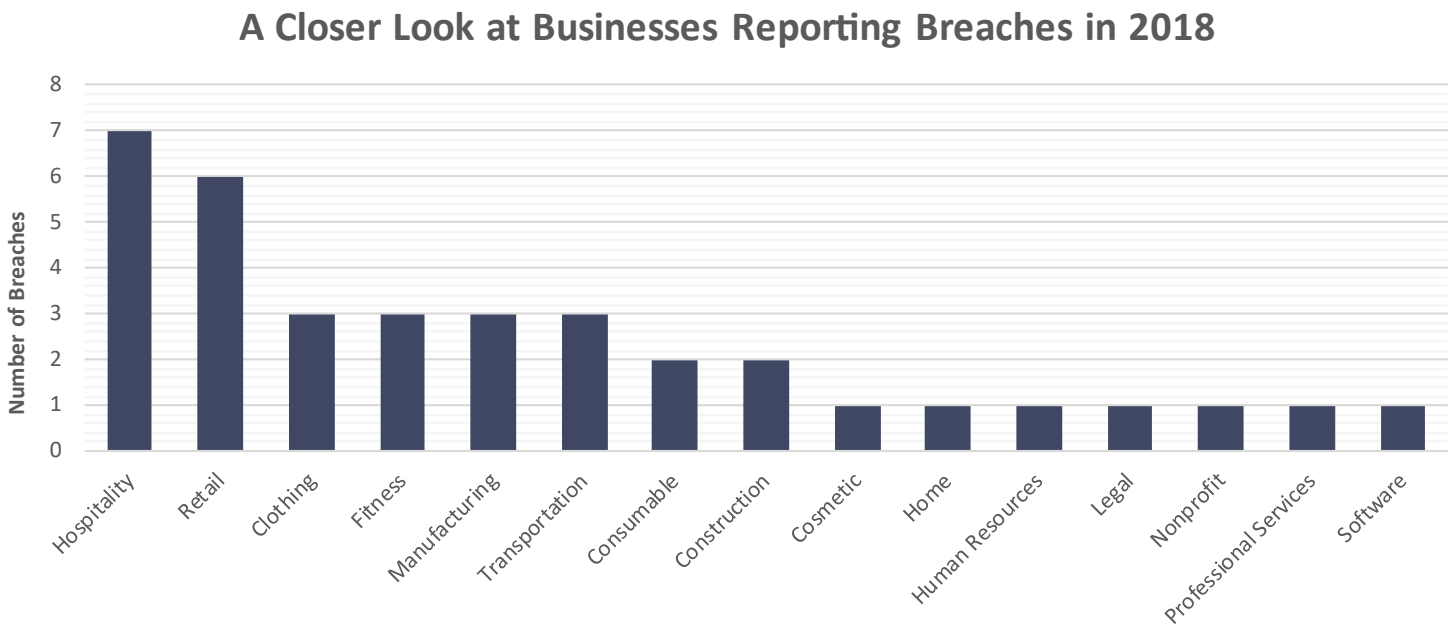
The Attorney General's Office tracks breaches by industry. Consistent with earlier reports, the office uses industry categories based on the Identity Theft Resource Center's classifications, including:

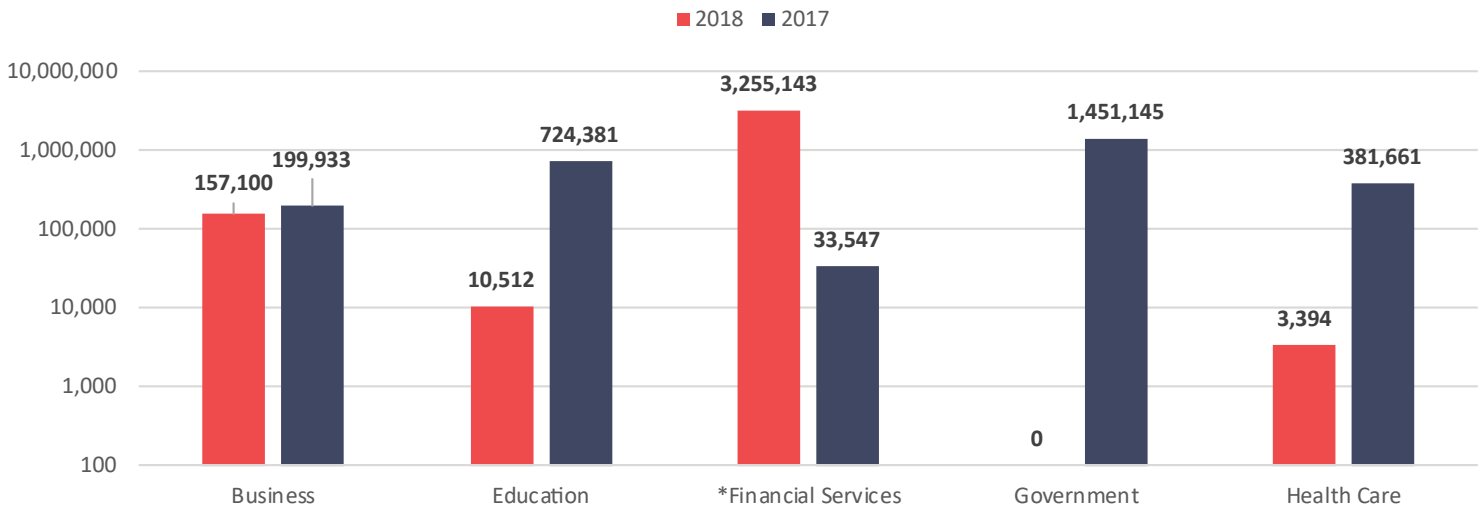
- Business;
- Education;
- Financial services;
- Government; and
- Healthcare.

The business category includes 21 sub-categories, including retail, nonprofit, transportation, human resources, hospitality, manufacturing, and software.

Continuing the trend from 2017, the majority of breaches reported in 2018 came from organizations categorized as businesses, which accounted for over 70% of all breaches. Malicious cyberattacks were responsible for more than half of these data breaches, most commonly through phishing e-mails and installation of malware on point-of-sale systems. Hospitality and retail represented just over a third of all the breaches among businesses in 2018.

Industries Reporting Breaches





*The 2018 data for Financial Services includes the Equifax, Inc. breach reported Sept. 7, 2017, which affected 3,243,664 Washingtonians. Excluding the Equifax breach, the financial services industry represented 11,479 compromised records for the time period of July 24, 2017 to July 23, 2018.

Businesses experienced an increase in the average number of records compromised per breach from 3,772 in 2017 to 5,611 in 2018 – nearly a 50% increase. Despite this, organizations categorized as businesses accounted for only 4.6% of the total number of records compromised in Washington state. This is due to the single massive breach of data held by Equifax, which is categorized for the purposes of this report as a financial services organization.

Excluding the Equifax breach, businesses accounted for 86% of the records compromised in 2018.

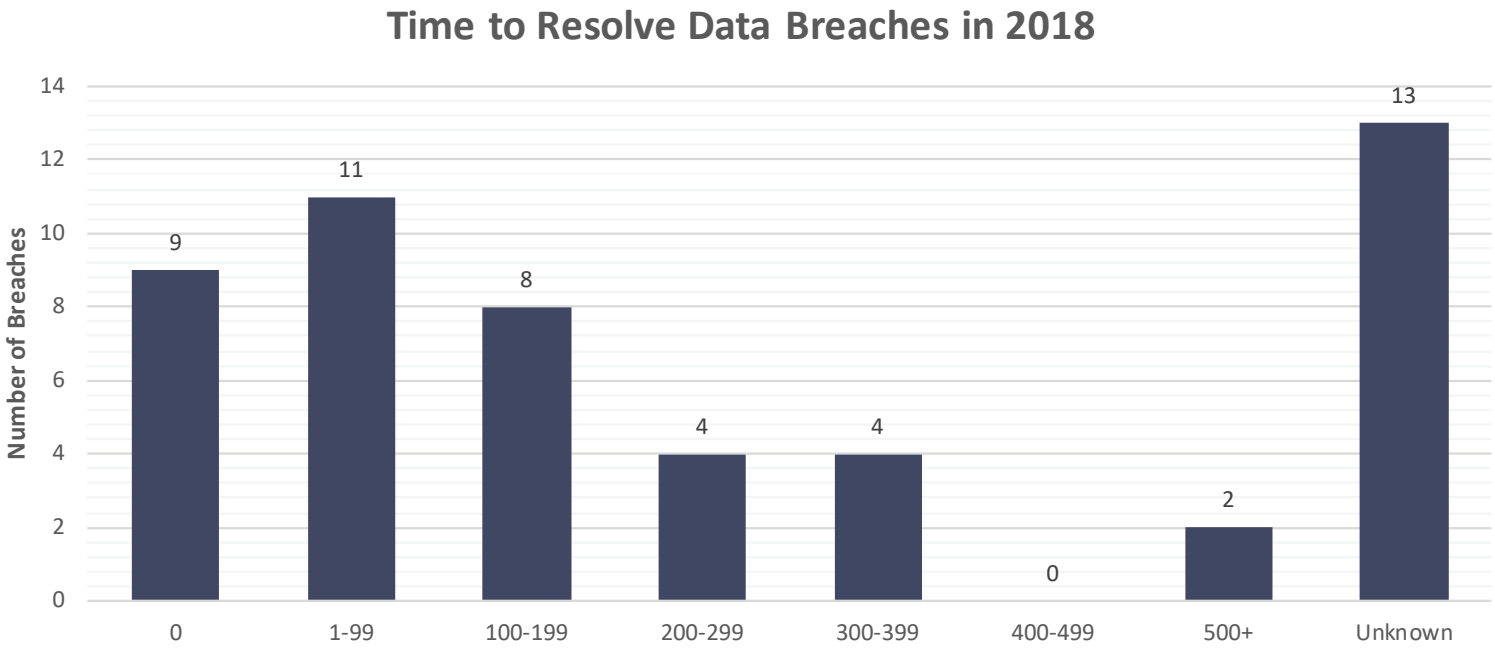
Impact of Data Breaches on Washington Businesses

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 a risk for all businesses.

According to a national study by the Ponemon Institute, the average cost of a data breach to an American business in 2018 is $233 per compromised record, up 3.6% from 2017.[2] The study found that, of the $233 per compromised record, $152 relates to indirect costs, such as turnover of customers resulting from the breach, and $81 comes directly from the breach, including legal fees, credit monitoring services for consumers, and security improvements.

Consistent with breaches reported in Washington, the study also found that, globally, malicious attacks are the primary cause of data breaches – approximately 48% of the cases – and are the most expensive type of data breaches for businesses.

Time to Resolve Data Breaches



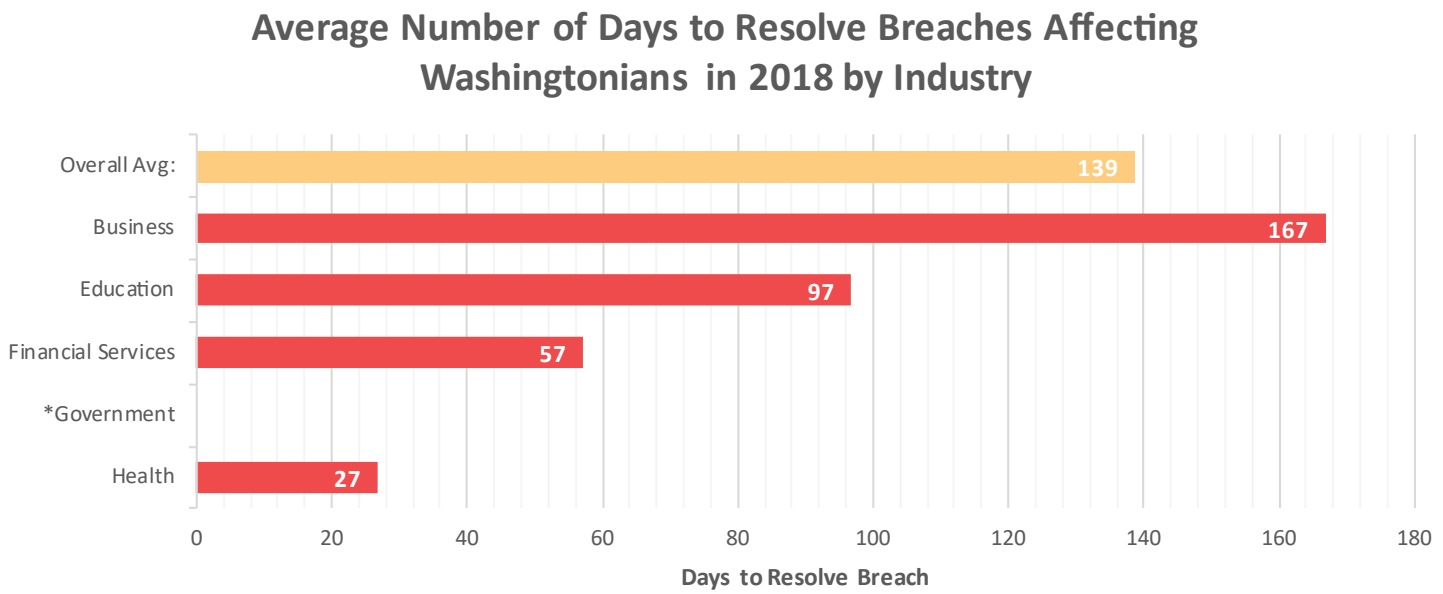
What Does It Mean to Resolve a Breach?

Resolution of a breach involves two steps: identification and containment. In this report, identification is measured as the number of days that pass between the time when the data breach occurs and discovery of the breach 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.

The majority of data breaches in 2018 took less than 100 days to resolve. There were 13 breaches in 2018 where the dates of identification and containment were not specified in the notification. This was the most for any of the below categories – representing an average of 13,809 records per breach. This number is down significantly from 2017, when the average was 212,989 records per breach for this category. However, the "Unknown" category still represents the second highest average of records per breach in 2018.

Time to Resolve Data Breaches

On average, breaches reported to the Attorney General's Office in 2018 took 135 days to identify, and seven days to contain. In many cases, the discovery of a breach occurred after the breach had ended, meaning it took zero days to "contain" that breach. However, there were some significant exceptions. For instance, Bulletproof 360, Inc. (a manufacturer of coffee and tea products, and dietary supplements) reported a breach in September 2017 that resulted from a malicious cyberattack when unauthorized code was inserted into the software that operates its website's checkout page. After discovering the breach, it took Bulletproof 360, Inc. an additional 75 days to secure access to the affected information.



*No qualifying breaches were reported for Government in 2018

How Long Did Business Take to Identify & Contain Breaches?

According to the Ponemon Institute, globally, if a business identified a data breach in under 100 days, the estimated average total cost of the data breach was $3.11 million.[3] However, if it took more than 100 days to identify the breach, the estimated cost was $4.21 million. On average, the organizations included in the Ponemon study took 197 days to identify a breach, and 69 days to contain it. In 2018, we saw similar averages in Washington.

Among the breaches reported to the Attorney General in 2018, it took companies in the business category longer to resolve a breach than any other industry, with an average of 167 days per breach. That is 70% longer than the next closest industry, education, which on average took 97 days to resolve a breach. Of the 36 businesses reporting data breaches to the Attorney General's Office in 2018, 29 specified the amount of time it took them to discover the data breach. Of those 29, less than half reported that they had discovered the data breach in fewer than 100 days after it had begun.

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 affects 500 or more Washington residents.

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.

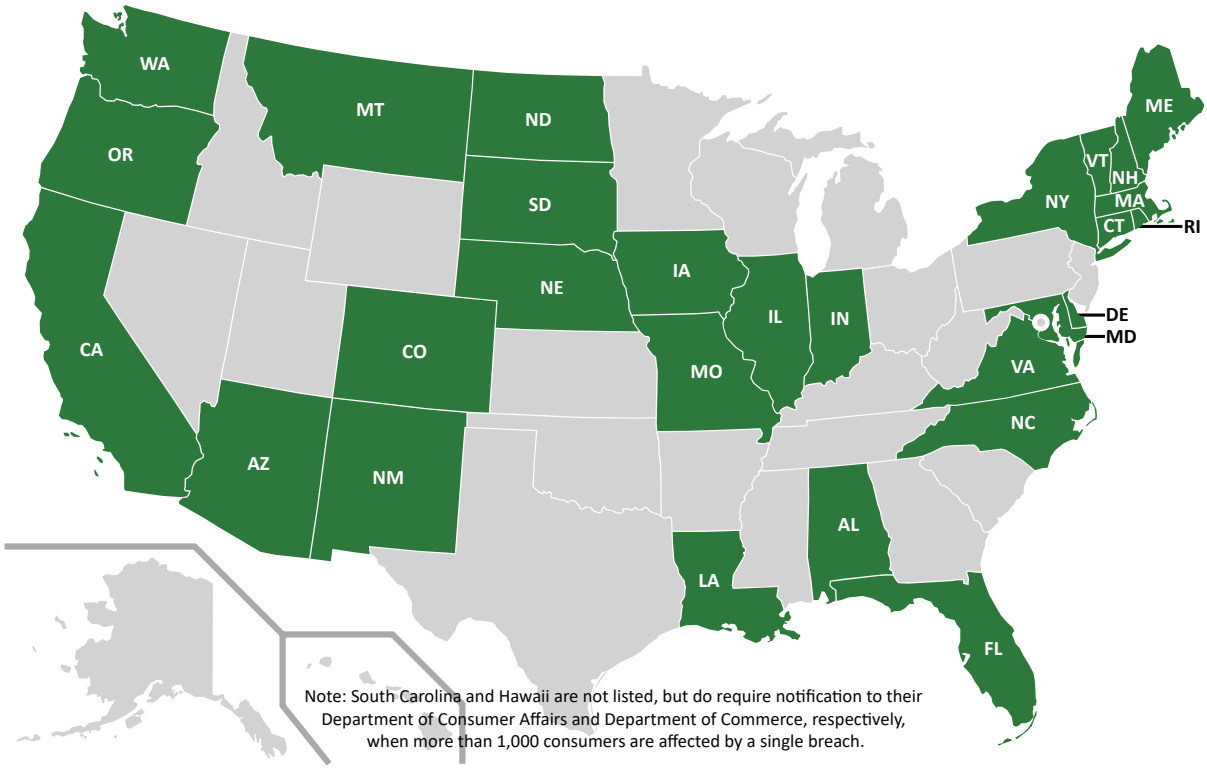
How Does Washington Compare to Other States & Global Trends?

Washington Compared to Other States

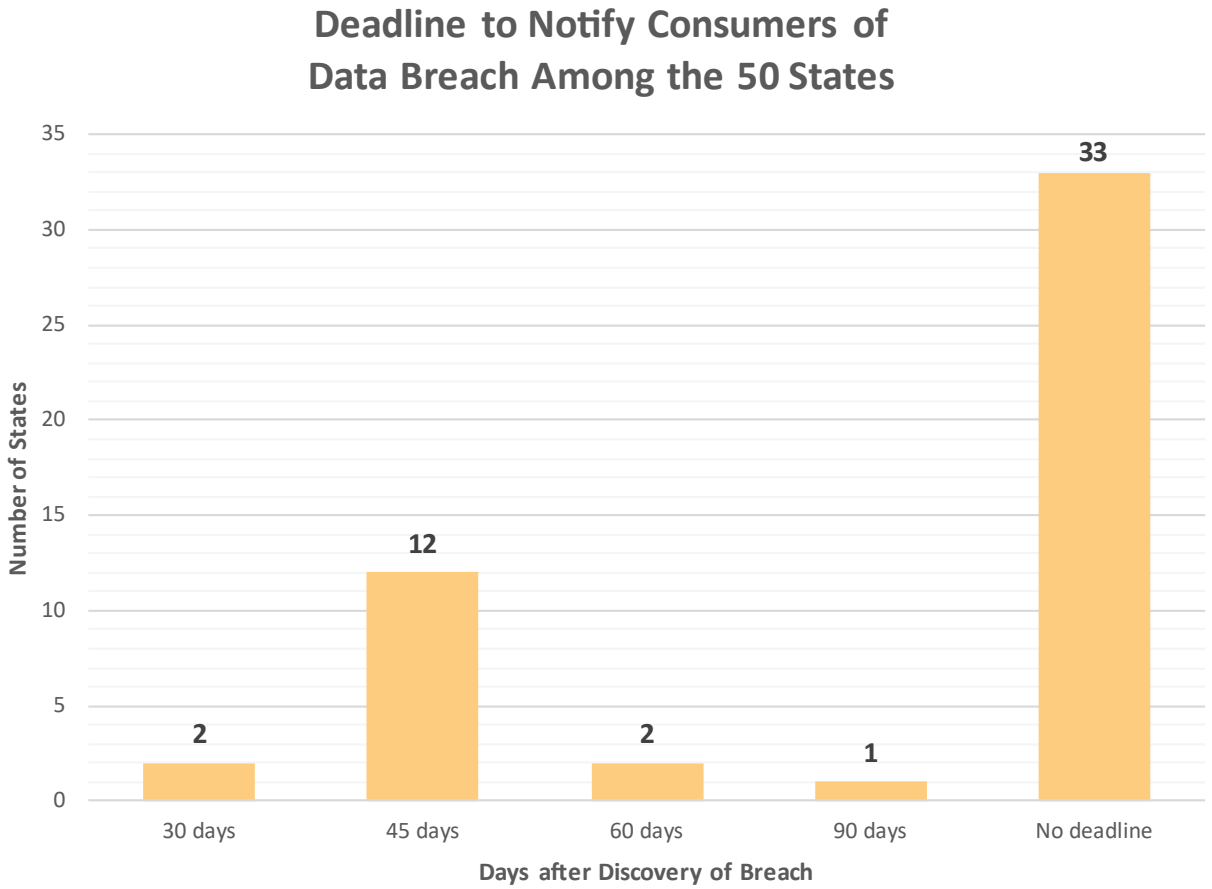
Currently, all 50 states have laws requiring private or governmental entities to notify individuals when a data breach occurs.[4]

In all 50 states, notification of individuals is not required if the information compromised was encrypted, redacted, or otherwise unreadable. However, in 24 states, including Washington, notification is required when an encryption key or security credential that could render the personally identifiable information

States Requiring Notification of State Attorney General Upon Discovery of a Data Breach (2018)



Note: South Carolina and Hawaii are not listed, but do require notification to their Department of Consumer Affairs and Department of Commerce, respectively, when more than 1,000 consumers are affected by a single breach.



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

In 28 states, including Washington, entities experiencing a breach must notify the Attorney General. South Carolina and Hawaii require notification to their Department of Consumer Affairs and Department of Commerce, respectively, when more than 1,000 individuals are affected by a single breach.

In 16 states, including Washington, notification that a breach has occurred must be provided to affected individuals by a specific deadline. In 12 states, including Washington, the deadline is 45 days. Florida and Colorado require notification to individuals and the Attorney General within 30 days, and Vermont – in addition to a 45-day deadline to notify individuals – requires notification of the state's Attorney General within 14 days of discovering a breach. Most states with a deadline, including Washington (RCW 19.255.010 (16)), 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."[5]

Defining Personally Identifiable Information

Most states, including Washington, use the same general definition of "personally identifiable information":

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 definitions of personally identifiable information. Additional elements beyond those contained in Washington's law include:[6]

Data Element	States That Include the Data Element in Their Definition of Personally Identifiable Information
Date of birth	**North Dakota**
Digital signature	**North Carolina, North Dakota**
DNA profile	**Delaware, Wisconsin**
Health insurance policy number, or any unique identifier or subscriber identification number used by a health insurer to identify individual consumers	**Alabama, Arizona, Colorado, Florida, Maryland, Missouri, Nevada, Oregon, Virginia**
Medical/health information, such as medical history, treatments or diagnoses, and mental or physical condition	**Alabama, Arizona, Arkansas, California, Colorado, Delaware, Florida, Illinois, Maryland, Missouri, Montana, New Hampshire, North Dakota, Oregon, Rhode Island, South Dakota, Texas, Virginia, Wyoming**
Military identification number	**Alabama, Colorado, Florida**
Passport identification number	**Alabama, Arizona, Colorado, Delaware, Florida, Louisiana, Maryland, Oregon**
Student identification number	**Colorado, New Hampshire**
Taxpayer identification number	**Alabama, Arizona, Delaware, Maryland, Montana, Virginia**
Unique biometric data used to authenticate an individual when accessing an account, including fingerprints, voice prints, iris or retina patterns, facial characteristics, and hand geometry	**Arizona, Colorado, Delaware, Iowa, Illinois, Louisiana, Maryland, Nebraska, New Mexico, North Carolina, Oregon, South Dakota, Wisconsin**
Username or e-mail address in combination with a password or security question and answer	**Alabama, Arizona, California, Colorado, Delaware, Florida, Illinois, Maryland, Nebraska, Nevada, South Dakota**

GDPR – What is it & What Does it Mean for Washingtonians?

In the European Union (EU), the General Data Protection Regulations (GDPR) went into effect on May 25, 2018. Whereas Washington law and this report focus on what happens after data breaches occur, the GDPR establishes data security and privacy laws to focus on prevention of data breaches. This includes statutes regulating the rights of individuals to consent before having their data collected, to have easier access to the data that companies currently hold about them, and to request the erasure of certain personal data elements from a company's database.[7]

Washington state does not currently have laws equivalent to the GDPR. However, Washington businesses and individuals have been impacted by the regulations set out in the GDPR, because the GDPR applies globally to any entity that collects personally identifiable information data on EU consumers. As a result, many U.S. digital companies, non-profit organizations, service providers, and webmasters have started to implement changes to their privacy policies globally, in order to minimize overhead and potential liability in complying with the GDPR.[8]

The GDPR also contains requirements related to data breach notifications. As opposed to the common 45-day deadline in the United States, the GDPR requires notice to the appropriate "supervisory authority" within three days of discovering that a data breach has occurred.[9]

Conclusions & Recommendations

Data breaches and identity theft continue to be a significant threat to Washington residents, businesses, and agencies. Although fewer data breaches were reported in 2018 than in 2017, the total number of affected Washingtonians increased by more than 700,000 individuals.

To strengthen protections for Washingtonians in the face of these growing threats, our office makes the following recommendations to policymakers:

1. **Reduce the deadline for notice to affected Washingtonians to 30 days after discovery of a breach.**

In 2015, the Attorney General's Office requested legislation to strengthen the state's data breach laws by requiring entities to provide notice to affected Washingtonians within 30 days of discovering a breach. Ultimately, the Legislature passed the AG-request legislation with an amended 45-day deadline.

In 2015, Florida was the only state with a 30-day notice requirement. This summer, recognizing the increasing threat of data breaches to its residents, Colorado's legislature voted unanimously in both chambers to approve a data breach notification law requiring notice 30 days after discovery of a breach.[10] The Washington Legislature should join Florida and Colorado by reducing Washington's notification deadline to 30 days.

A reduced notification deadline limits individuals' exposure to risks of identity theft and other adverse impacts by making them aware of the breach earlier so they can take appropriate precautionary measures to protect their data.

2. **Require a preliminary notification to the Attorney General's Office within ten days of a breach's discovery so that the Attorney General's Office can alert the public more quickly of potential risks to its information through Consumer Notices.**

Washingtonians deserve to know about potential threats to the security of their data as soon as possible. A 30-day deadline still has the potential to keep individuals unaware of risks to their information for multiple weeks. Requiring a preliminary notice to the Attorney General's Office within 10 days of the discovery of a breach will allow the Attorney General to disseminate Consumer Notices and Alerts to inform the public about a breach. Washingtonians deserve the earliest possible opportunity to consider precautionary measures.

3. **Require entities to provide information about the timeline of a breach in their notices to affected individuals and the Attorney General's Office.**

In 2018, 13 organizations reported breaches to the Attorney General's Office without providing dates for the start of the breach, the end of the breach,

when the breach was discovered, or when the breach was contained. In short, these entities provided the Attorney General's Office no way of knowing how long the personal information of Washingtonians was compromised in each of these breaches.

For notifications to be maximally effective, it is critical that Washingtonians and policymakers have complete information about when data breaches occur and how long personally identifiable information was compromised. The Attorney General's Office needs this information to properly inform policymakers, businesses, and the public about the magnitude of the challenges associated with data breaches, and to help individuals determine if their information is at risk.

4. Expand the definition of Personally Identifiable Information.

Washington state's data breach notification law includes a narrow definition of personally identifiable information. Consequently, if a malicious hacker obtains sensitive information about an individual, such as the combination of an email address and password, notice is not required to that individual, even though their sensitive information was exposed.

Other states have expanded their definition of personal information to include several additional categories of sensitive data (see: "How Does Washington Compare to Other States & Global Trends?" above for details). To strengthen protections for Washingtonians, the Legislature should expand our state's definition of personal information to include an individual's:

- Full date of birth;
- Username or e-mail address in combination with a password or security question;
- Digital signature;
- DNA profile, or other forms of biometric data; and
- Health insurance, military, passport, or student identification number.

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. RCW 19.255.010, effective since July 2015.

2. “2018 Cost of a Data Breach Study: Global Overview,” Ponemon Institute, July 2018.

3. Ibid.

4. “Security Breach Notification Laws,” National Conference of State Legislators, April 12, 2017. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

5. “Data Breach Charts,” BakerHostetler, July 2018.

6. Ibid.

7. General Data Protection Regulation (EU) 2016/679, Chapter 3. https://gdpr-info.eu/chapter-3/

8. “A practical guide to the European Union’s GDPR for American businesses,” Recode, May 16, 2018. https://www.recode.net/2018/5/16/17360944/gdpr-us-business-eu-european-union-data-protection-privacy

9. General Data Protection Regulation (EU) 2016/679, Chapter 4, Article 33. https://gdpr-info.eu/art-33-gdpr/

10. Colorado's bi-partisan sponsored bill, HB18-1128 "Protections For Consumer Data Privacy," was approved by a vote of 66-0-5 in the House and 33-0-2 in the Senate. Details on the bill and the vote can be found at https://leg.colorado.gov/bills/hb18-1128