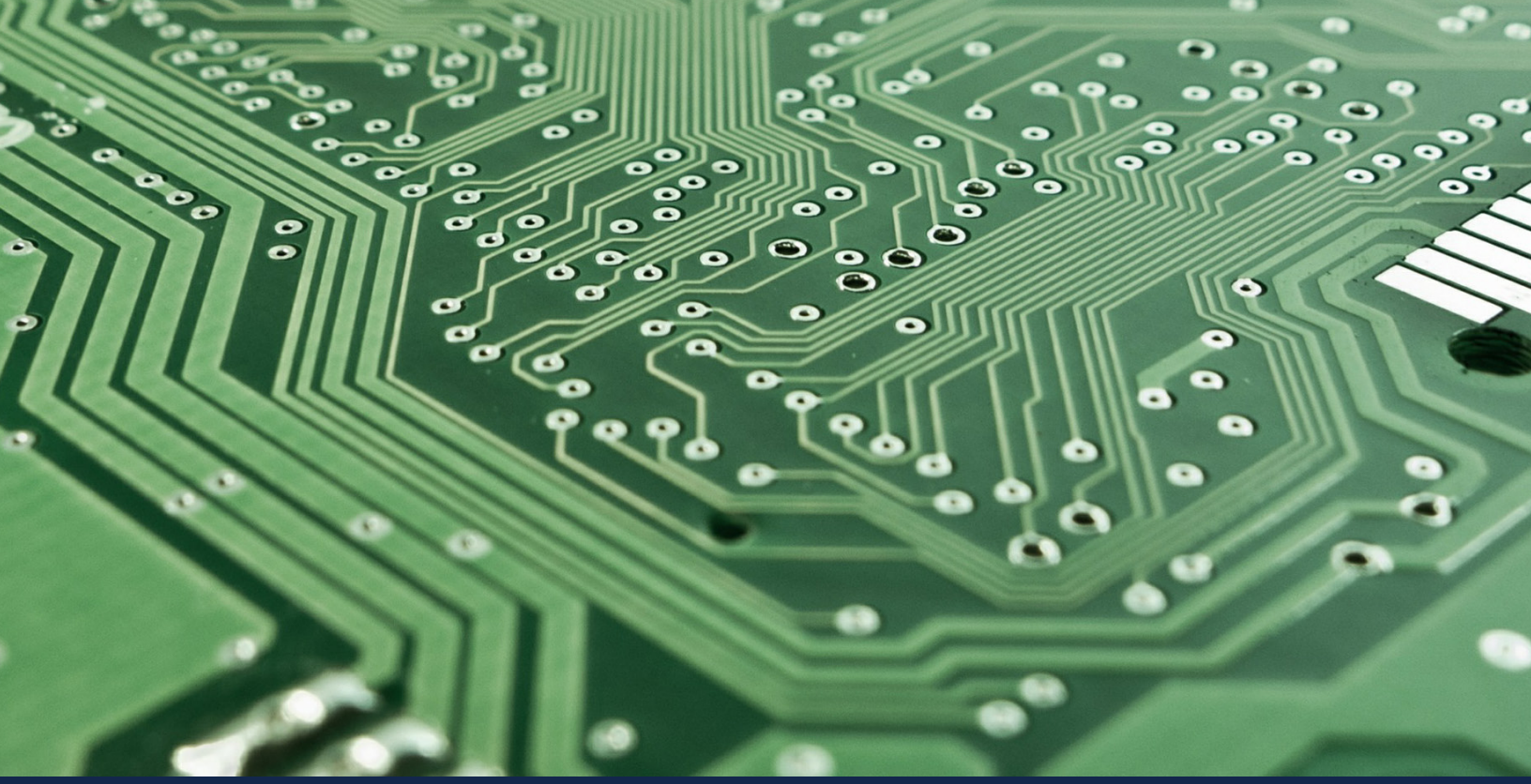
WASHINGTON STATE ATTORNEY GENERAL'S OFFICE

2017 DATA BREACH REPORT



Report Contents:

October 2017

Dear Washingtonians,

Data breaches are a significant threat to both businesses and individual consumers. Recently the Equifax data breach exposed the personal data of 143 million Americans. This is a sobering reminder of the importance of data security.

This is the second edition of the Attorney General's Office Annual Data Breach Report. In 2015, the Washington Legislature updated our data breach notification laws ensuring my office receives notice whenever a data breach potentially exposes personal information. This allows my office to be a data breach watchdog.

Over the past year, 78 reported data breaches compromised the personal information of more than 2,700,000 Washington residents. This is a significant increase from 2016, when my office was notified of 39 breaches affecting the personal information of more than 450,000 Washingtonians. This increase reflects an alarming trend. Businesses and governments must take steps to secure the data they possess.

Data breaches occur in organizations of all types, including hotels and fitness companies, financial service companies and universities. Similarly, there is a wide variety in the way data breaches can occur. In one case, an individual pretending to be the business owner emailed a request for all 2016 W-2 forms prepared by the company. The records were provided before the company discovered the request came from a fraudulent account.

I am working with other state attorneys general to ensure that businesses take necessary steps to protect consumers' personal information and to investigate and hold businesses accountable when their security measures fall short.

In November 2013, data held by the Target Corporation was breached when cyber attackers gained access to a customer service database, installed malware on the system and captured consumer data. The breach compromised the personal information of millions of consumers. Target entered into a binding agreement to resolve an investigation by Washington and 46 other state attorneys general. The agreement requires Target to develop, implement and maintain a comprehensive information security program and employ a person responsible for executing the plan. Target must also take additional measures to further strengthen the company's data security.

This report presents a summary of the data breach notices the Attorney General's Office received over the past year. You can find tips and resources for consumers and businesses at the end of the report. I hope you find this information helpful.

Sincerely,
Bob Ferguson
Washington State Attorney General

Executive Summary[1]

- Data breach notifications to the Attorney General's Office increased sharply from 39 in 2016 to 78 in 2017. A list of the data breach notifications received by the Attorney General's Office can be found at: http://www.atg.wa.gov/data-breach-notifications.

- Data breaches analyzed for this report affected over two and a half million records containing personally identifiable information, far more than the 450,000 records affected in 2016.[2]

- Many of the findings in the 2016 Report are also true in 2017:
  - The majority of data breaches reported to the Attorney General's Office affected fewer than 10,000 Washington residents;
  - Payment card information was the most commonly compromised type of personal information, followed by name and address;
  - Malicious cyberattacks were the most common cause of data breaches affecting Washington consumers; and
  - A single data breach resulted in the exposure of more records than all other breaches combined.[3]

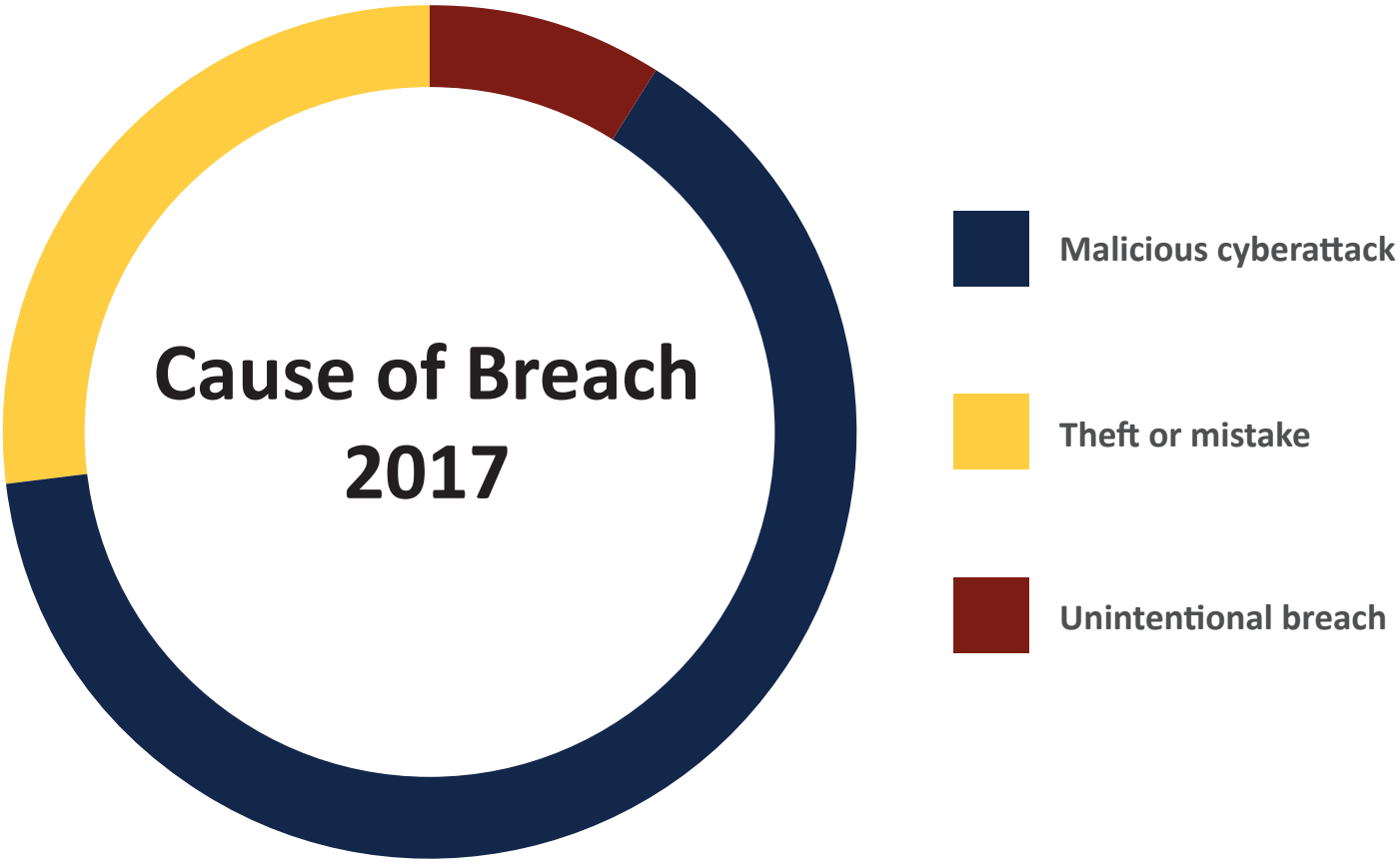
- Based on information compiled in this report, the Attorney General's Office makes the following recommendations:
  - Businesses must work harder to identify and resolve data breaches more quickly.
  - Governments must do a better job of securing data, including strengthening their own data security and ensuring government contractors adequately secure personal consumer information.
  - Policy makers should **should consider whether a 45-day deadline for notice sufficiently protects consumers, and whether a shorter deadline for notice to the Attorney General's Office is appropriate.**

Causes of Data Breaches

- Nearly two-thirds of Washington data breaches in 2017 were a result of cyberattacks. This is an increase over 2016, when nearly half of data breaches were caused by cyberattack.

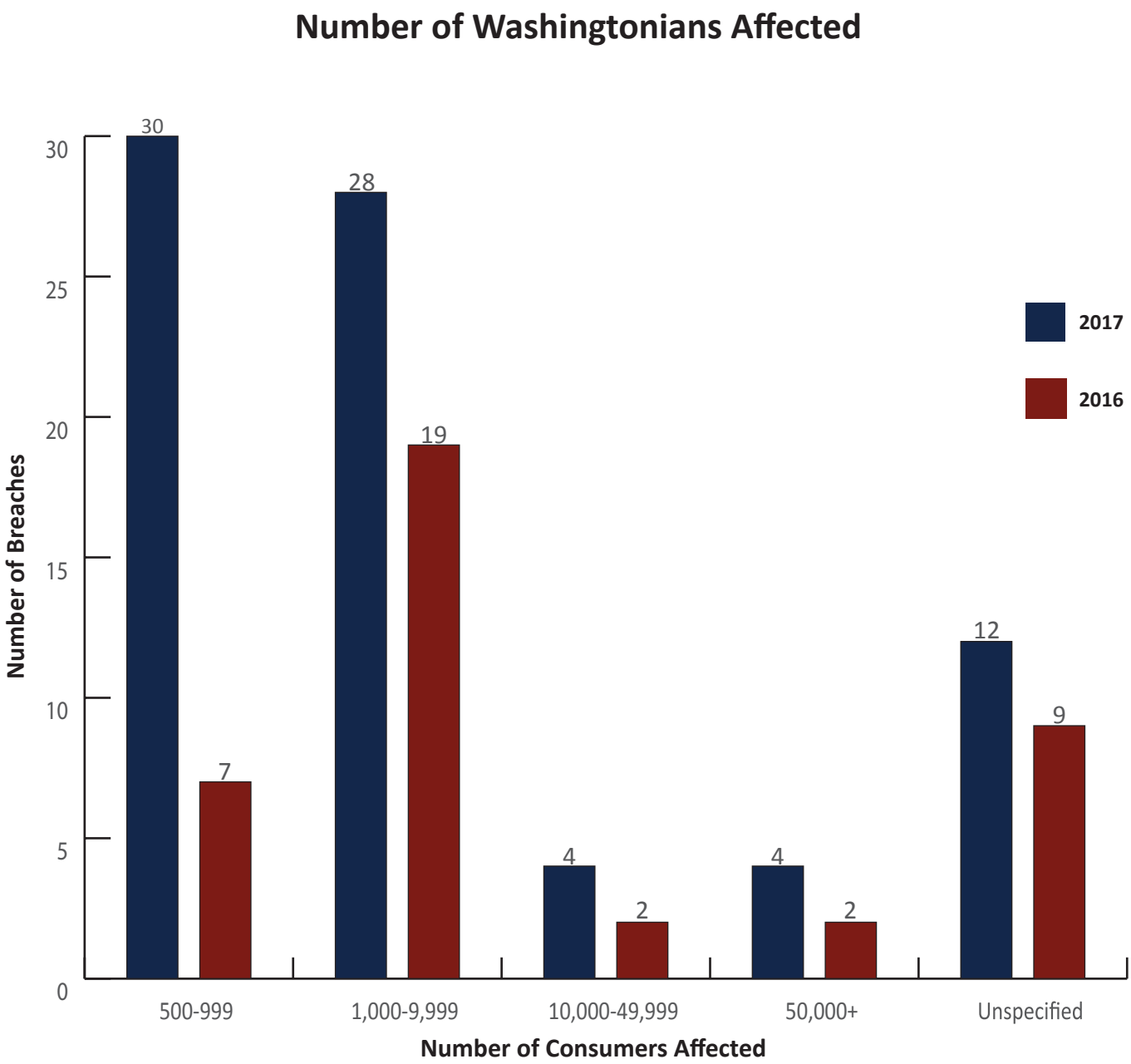
- There are three broad categories of causes of data breaches:
  - *Malicious cyberattack*: When a third party deliberately attempts to gain or succeeds in gaining access to secure data stored on a server. The attack can use a virus, malware, phishing email, or similar means of accessing secure data.
  - *Theft or mistake*: This category includes the loss or theft of information, such as the theft of a laptop containing patient medical records or a clerical error that sent W-2 information to an unintended recipient.
  - *Unauthorized access*: When an unauthorized person accesses secure data through means such as an unsecured network.

Cause of Data Breach	Number of 2017 breaches	Percentage of 2017 breaches	Number of 2016 breaches	Percentage of 2016 breaches
Malicious cyberattack	50	64.10%	19	48.72%
Theft or mistake	21	26.92%	16	41.03%
Unintentional breach	7	8.97%	4	10.25%



Number of Washingtonians Affected

- In 2017 there were 78 data breaches, affecting 2.7 million Washingtonians.
- The majority of data breaches compromised the personal information of 500-999 residents.
- The number of data breaches affecting 500-999 people is significantly higher than during 2016.
- ACTIVE Outdoors was an outlier; it had a breach of information of nearly 1.5 million individuals. More than half of the total number of Washingtonians affected by data breaches were affected by this breach, which was caused by unauthorized access of an unsecured server.
- There was an increase in data breach notifications for every range of number of affected Washington residents. Breaches affecting 500-999 residents had the largest increase compared to 2016.



Impact of Data Breaches

Businesses of all sizes are impacted by data breaches. Under Washington law, businesses have a responsibility to take reasonable steps to protect individuals' personal information. The variety of ways that data breaches can occur, including inadvertent disclosure, theft of hard copy information, and malicious cyberattacks, put all businesses at risk.

Over the past year, the Attorney General's Office received notifications of data breaches from a wide variety of businesses, including small retail businesses, arborist services and supplies, financial institutions, health insurers, health care providers, construction companies, hotel chains, individual hotels, and small tax preparers.

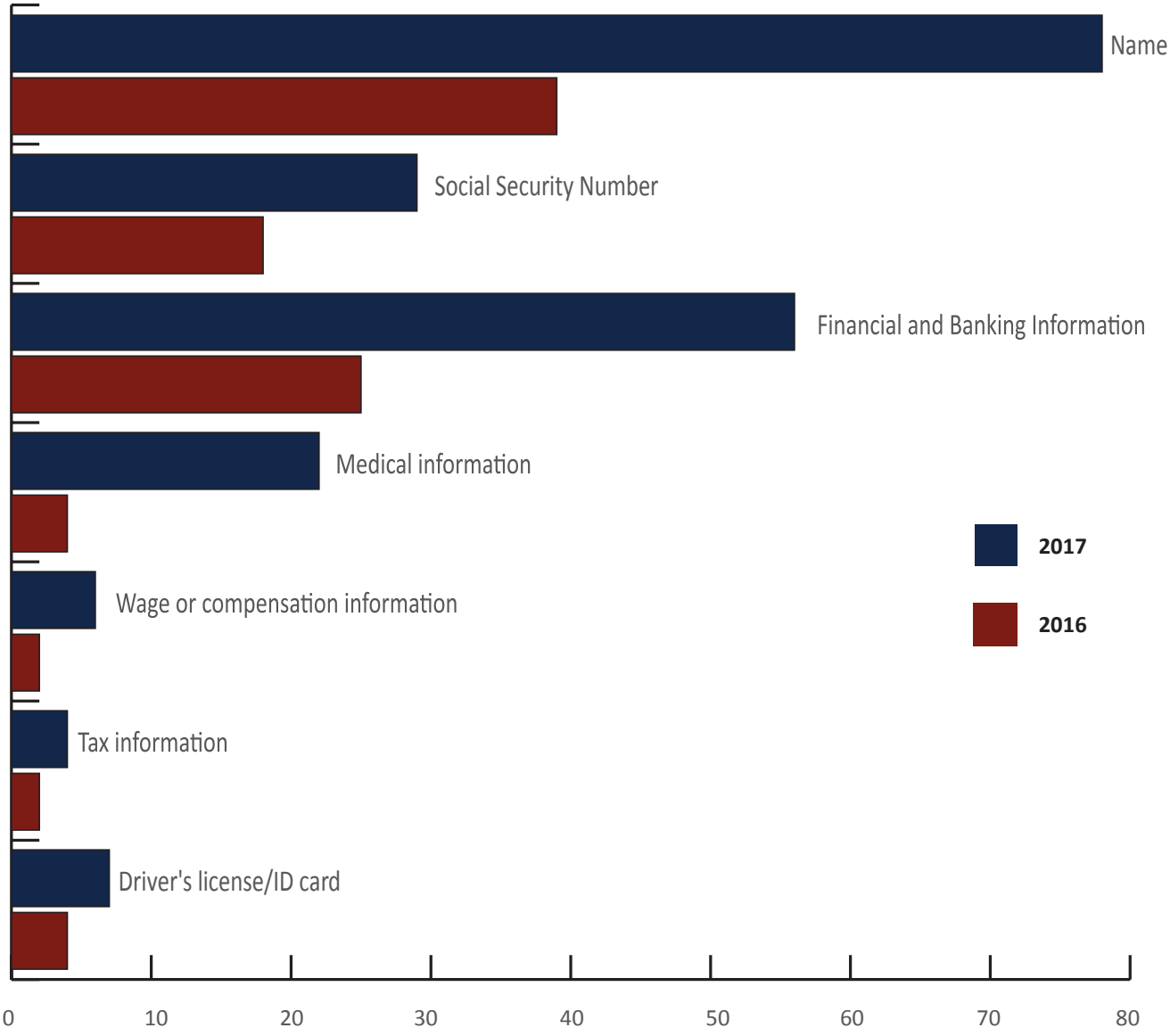
According to a national study by the Ponemon Institute, the average cost of a data breach to a business is $225 per compromised record.[5] Using this figure, data breaches compromising the personal information of Washington consumers likely cost businesses more than $500 million during the past year. The study found that, of the $225 per compromised record, $146 relates to indirect costs, such as turnover of customers resulting from the breach, and $79 directly relates to the breach, including legal fees, credit monitoring services for consumers, and security improvements.

Similar to the notices received by the Attorney General's Office, the study also found that malicious attacks are the primary cause of data breaches, and the most expensive type of data breaches for businesses. The companies included in the Ponemon Institute's study are all larger companies with access to sophisticated security.

The study also found that the more quickly a breach can be identified and contained, the lower the cost to the business.

Types of Personal Information Compromised

In both 2016 and 2017, financial information was the most commonly compromised type of personal information. Payment card information was typically acquired either through malware on online payment systems or through the use of skimmers in brick and mortar stores. Skimmers are devices that allow collection of payment information. Financial data were compromised in 56 of the 78 data breaches this year, totaling 208,216 individual financial records.



NUMBER OF BREACHES BY TYPE OF INFORMATION COMPROMISED

The law requires notification to the Attorney General's Office when the compromised data includes an individual's name in combination with any of the following:

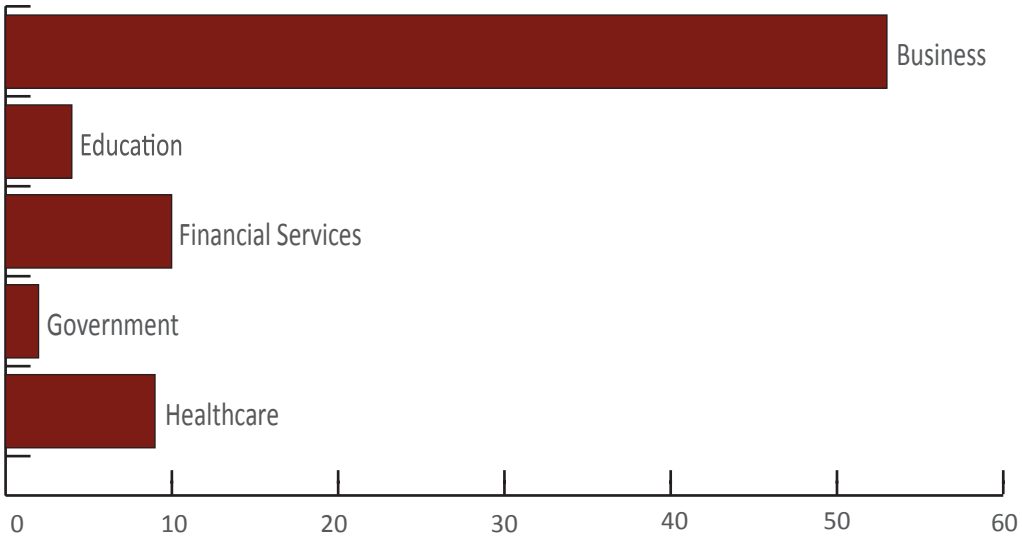
- Social Security number;
- Driver's license or Identification card number; or
- Banking or financial information, including payment card information.

The law also requires notification to the Attorney General's Office when personal health information covered by HIPAA is compromised.

Industries Reporting Breaches

Over two-thirds of the 2017 data breaches in Washington affected businesses. Malicious cyberattacks, especially malware installation on payment systems were the cause of the majority of the data breaches affecting businesses. Hospitality, entertainment and clothing businesses had the largest number of breaches affecting the business industry.

Number of Breaches by Industry

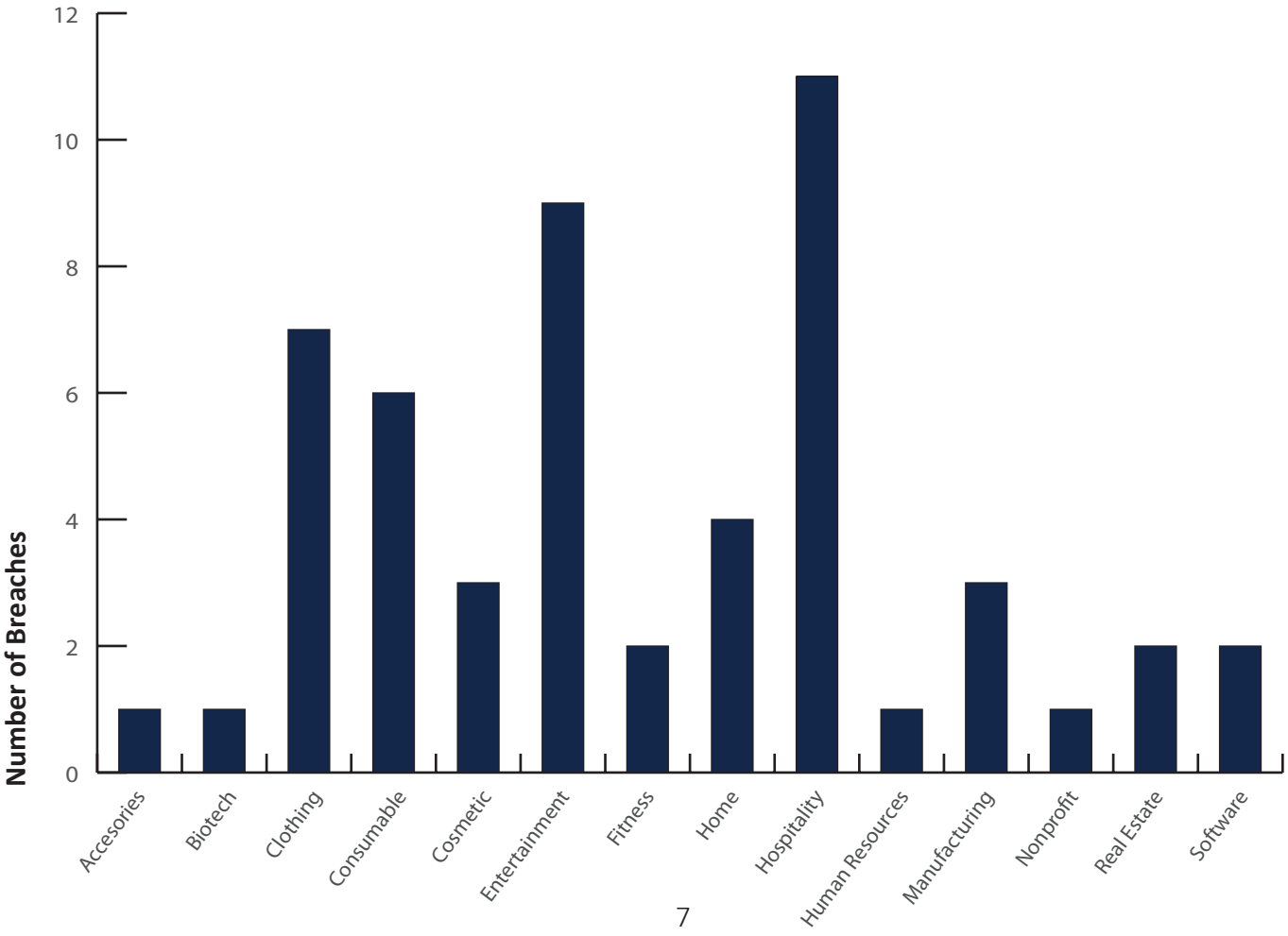


This year, the report uses industry categories based on the Identity Theft Resource Center's breach category classifications:

- business,
- education,
- financial services,
- government, and
- healthcare.

The business category includes retail, nonprofit, real estate, human resources, hospitality, manufacturing, and software companies.

A Closer Look at Businesses Reporting Breaches

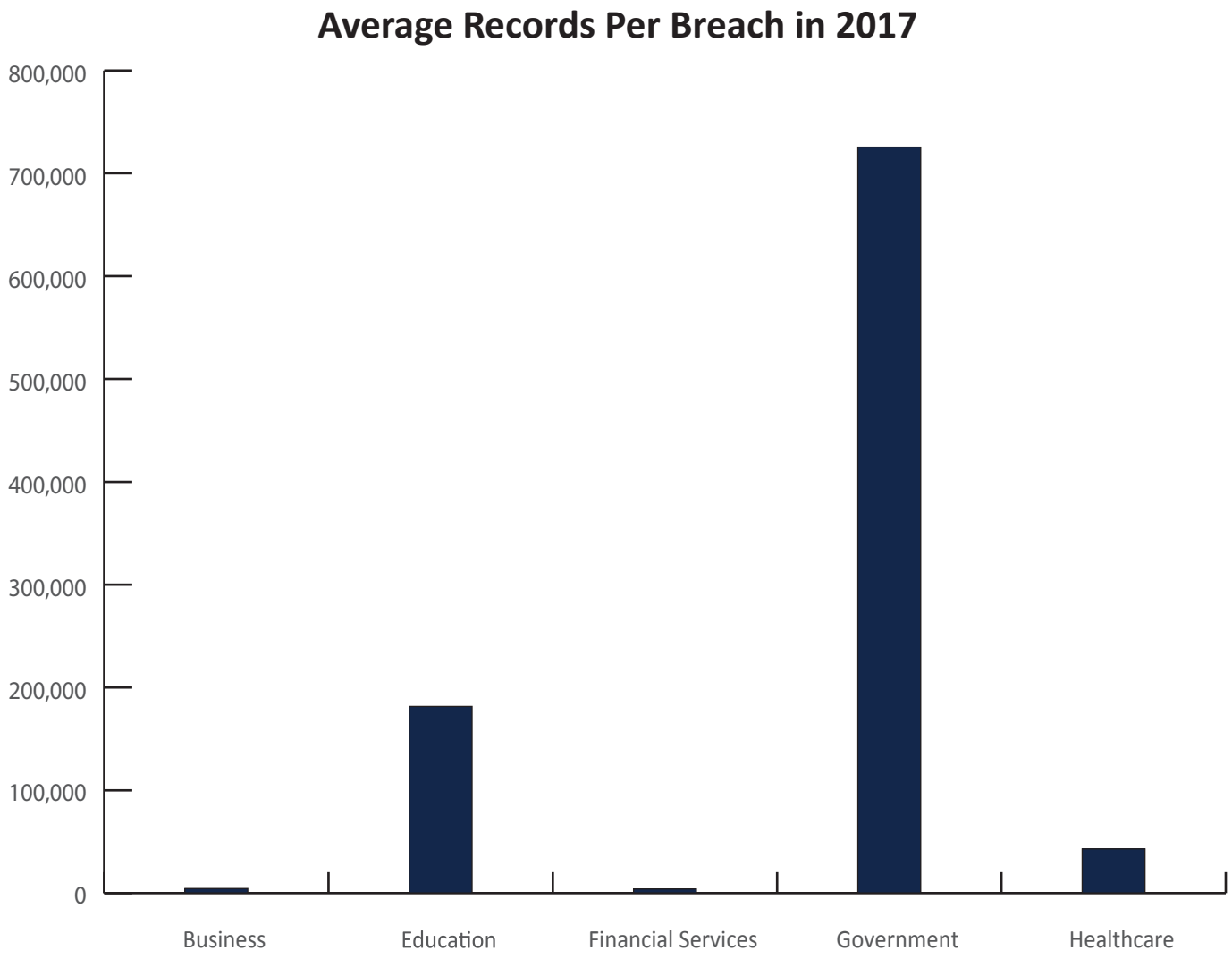


Industries Reporting Breaches

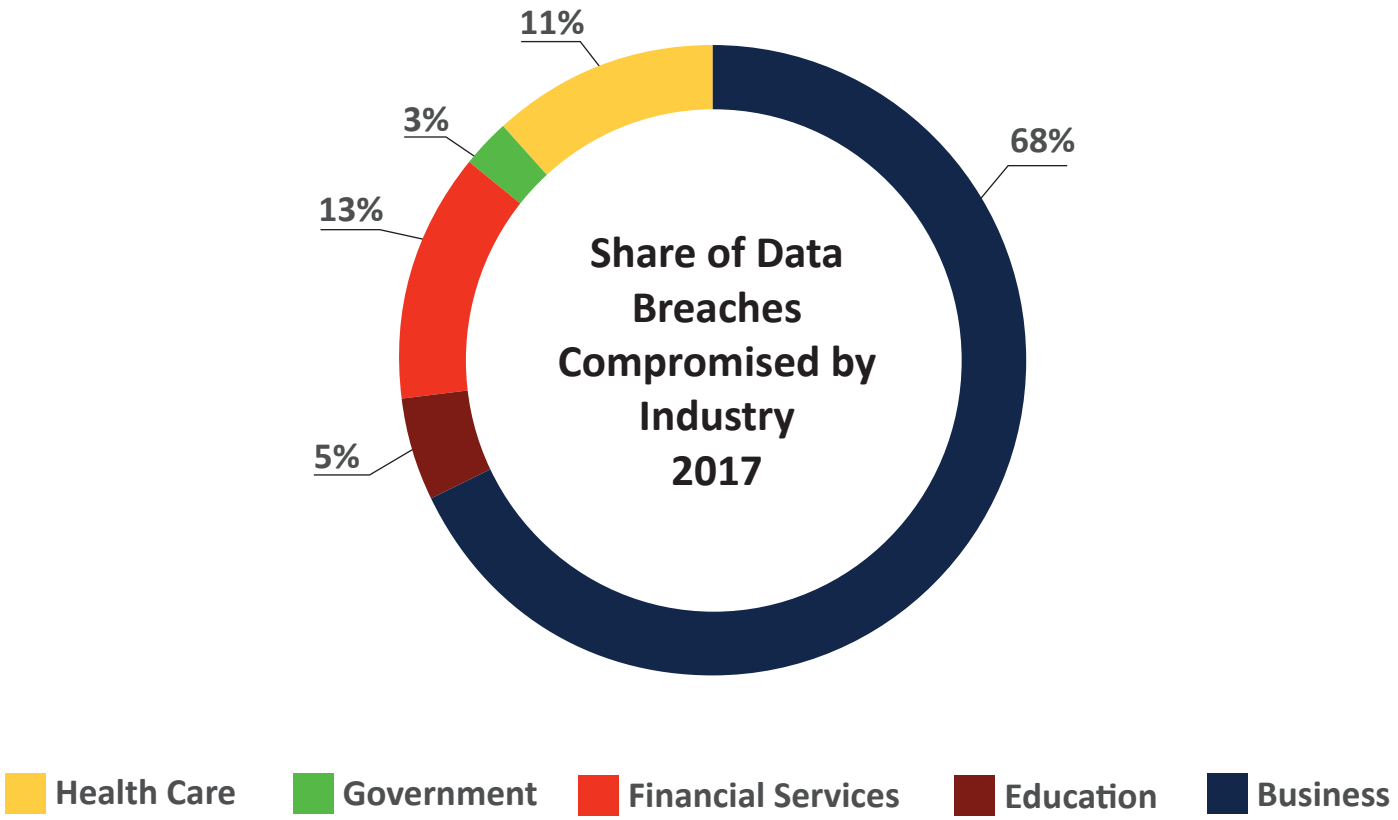
Business breaches accounted for 71% of 2017 data breaches, while government breaches accounted for 3%. However, business breaches accounted for only 7% of the number of records breached and government breaches accounted for 52% of all records compromised in 2017 data breaches.

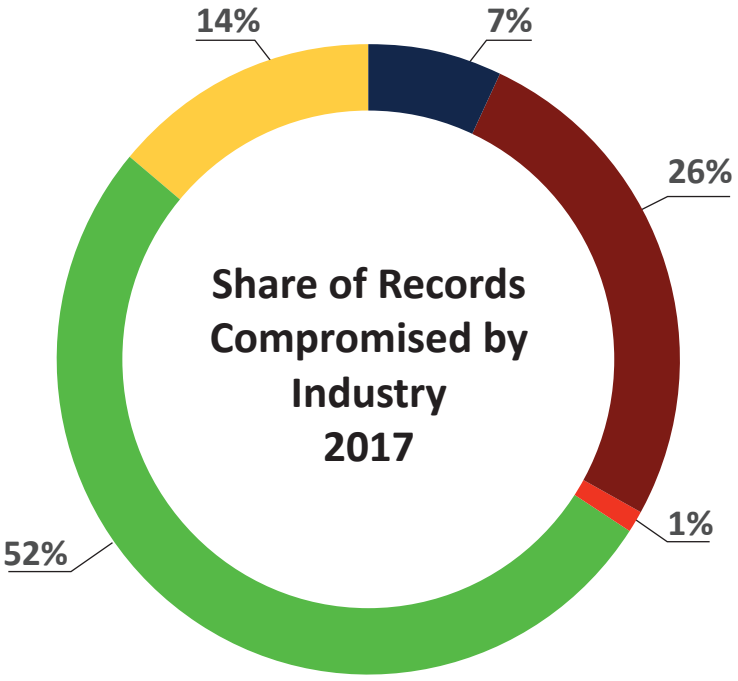
In 2017, data breaches of government records resulted in the greatest number of records compromised. The vast majority of these compromised records were the result of the ACTIVE Outdoors breach, which compromised the personal information of at least 1,449,645 Washingtonians. ACTIVE Outdoors hosted the online application system used to apply for or purchase state hunting and fishing licenses. Although ACTIVE Outdoors is not a government agency, this was categorized as a government breach because of the nature of the information that was exposed. Most consumers who purchased licenses through this system were not aware the system was operated by a third party. The information compromised included name, address, date of birth, and driver's license number, as well as physical description information, and in some cases, the partial Social Security numbers of Washington residents.

Recommendation: Governments must do a better job of securing data, including strengthening their own data security and ensuring government contractors adequately secure personal consumer information.



Industries Reporting Breaches



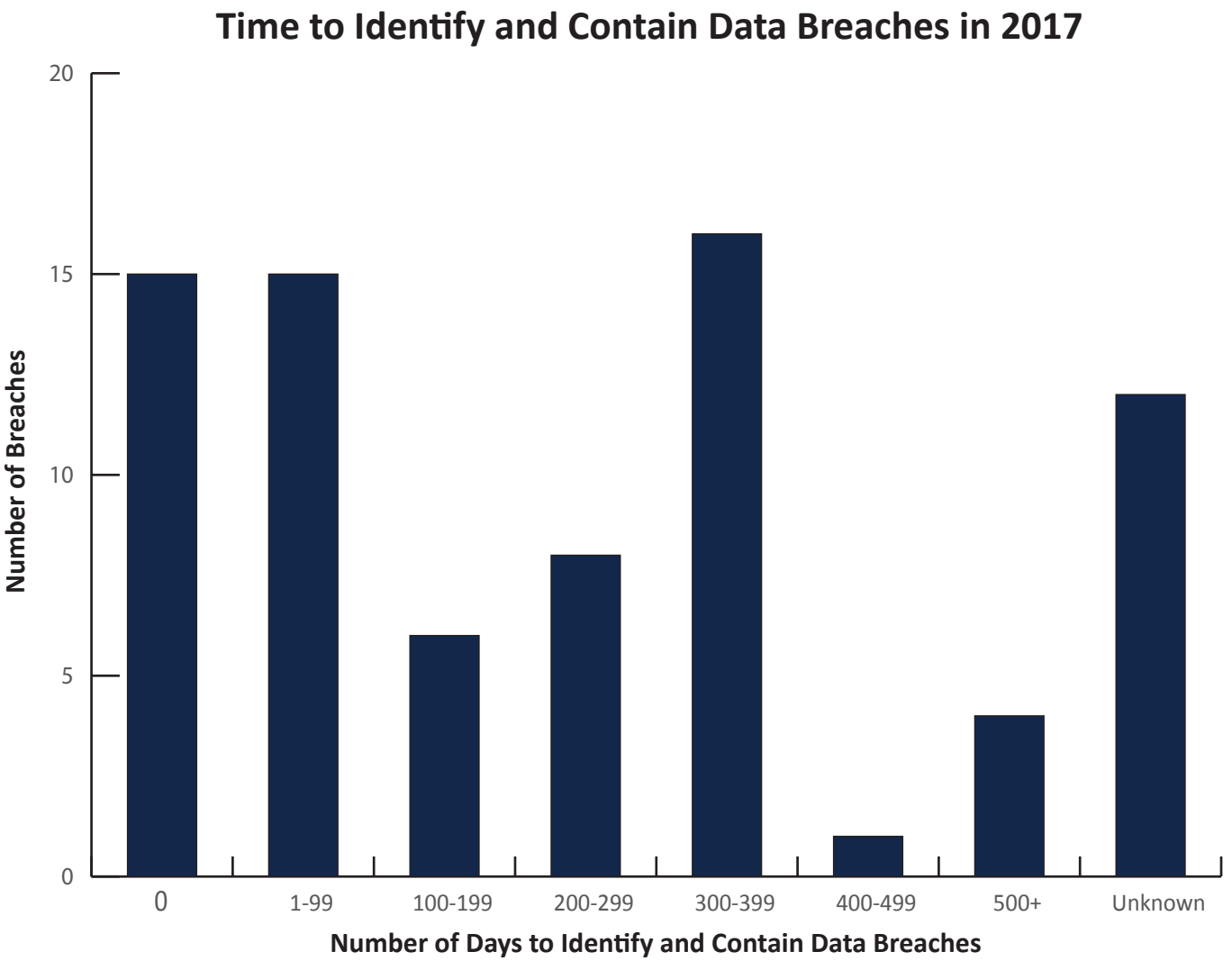


Time to Identify and Contain Data Breaches

The majority of 2017 data breaches took between 300 and 399 days to resolve, meaning the cause of the breach was identified and the information was secured. There were 12 breaches in 2017 where the number of days to identify and contain the breach was unspecified. These breaches had the highest number of records per breach at an average of 212,989 records per breach. A comparison to 2016 is not available because this metric was not analyzed in the 2016 report.

As noted earlier, the national study by the Ponemon Institute found that the more quickly a breach can be identified and contained, the lower the cost to the business. Of the 63 companies in the study that experienced data breaches, it took businesses an average of 191 days to identify and 66 days to contain the breach.[6]

Recommendation: Businesses must work harder to quickly identify and resolve data breaches.



Washington's Data Breach Laws

A data security breach, or 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. Data breaches are costly for the economy and can lead to individuals becoming victims of identity theft.

Notification

Businesses and public agencies are required to notify affected individuals when a data breach occurs, and notify the Attorney General's Office when a data breach affects 500 or more Washington residents.

Under the revised law, notification 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 notification laws, RCW 19.255.010 and RCW 42.56.590, cover "personal information." Personal information is defined as someone's first name or first initial and last name in combination with any of the following:

- Social Security number;
- Driver's license number or Washington identification card number; 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 an individual's account.

Entities covered by the Health Insurance Portability and Accountability Act (HIPAA) must also provide notification to the Attorney General's Office when a breach occurs involving health information covered by HIPAA. 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)).

Theft of Financial Information

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. This law is enforced by county prosecuting attorneys.

How Does Washington Compare with Other States?

Currently, 48 states have laws requiring that consumers receive notification when a data breach occurs.[7]

When is notification required?

- In 32 states, notification is not required if the information compromised was encrypted, redacted, or otherwise unreadable.
- In 15 states, including Washington, notification is required, even if the information compromised was encrypted, redacted, or unreadable, if the encryption key was obtained in the breach.
- Tennessee's statute does not exempt breaches of encrypted information.[8]

Is notification to the Attorney General required?

- In 25 states, including Washington, notification of a breach must be provided to the Attorney General. Maryland requires that the Attorney General be notified before notification is provided to consumers.

What is the deadline for notification after discovery of a data breach?

- In 11 states, including Washington, notification must be provided to consumers by a specific deadline. The most common deadline is 45 days, which is the requirement under Washington law. Florida requires notification to consumers and the Attorney General within 30 days.
- Most states, including Washington and other states that set a specific deadline, 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."

Recommendation: Policy makers should consider whether a 45-day deadline for notice sufficiently protects consumers, and whether a shorter deadline for notice to the Attorney General's Office is appropriate.

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 of identity theft.

If you suspect you are the victim of identity theft:

1. Call the companies where you know fraud occurred;
2. Work with one of the credit bureaus (Experian, TransUnion, and Equifax) to place a fraud alert or credit freeze on your credit report and receive a copy of your credit reports;
3. Report the identity theft to the FTC; and
4. File a report with your local police department.

Resources for Businesses to Protect Themselves

All industries and businesses are potentially susceptible to data breach. However, there are steps businesses can take to prevent a breach from happening. The Washington Attorney General's Office provides resources for businesses to protect against data breaches and to help explain the laws regarding data breaches and notifications. These resources are available at: http://www.atg.wa.gov/identity-theft-and-privacy-guide-businesses.

These basic steps can assist businesses in evaluating how well they are protecting personal information:

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.

Attorney General's Office Consumer Resource Center

800 5th Ave, Suite 2000
Seattle, WA 98104-3188
1-800-551-4636 (in state)
1-206-464-6684 (out of state)
1-800-833-6388 (relay service for the hearing impaired)
www.atg.wa.gov/consumer-protection

Photo Credits

Cover - Photo by Jannoon028 - Freepik.com

Notes

[1] The data represented in this report reflects the data breaches reported between July 24, 2016 and July 23, 2017. The data for this report were collected from the data breach notifications required by RCW 19.255.010 and RCW 42.56.590, available at: http://www.atg.wa.gov/data-breach-notifications. This report includes only notifications received that were required under Washington's notification law. Some businesses provided notification of breaches affecting fewer than 500 Washingtonians; these were not included. Other notices were omitted because they did not include "personal information" as defined in the law. Additionally, fourteen data breach notifications to the Attorney General's Office did not specify the number of Washingtonians affected, meaning a greater number of records were likely breached or susceptible to breach than reported here.

[2] There is a possibility that certain Washington residents were impacted by more than one breach. This number is the sum of records compromised by individual data breaches according to notifications submitted to the Attorney General's Office.

[3] The largest data breach involved unauthorized access to ACTIVE Outdoors' system used to store data for hunting/fishing licenses. The company reported that the information of nearly 1.5 million Washingtonians may have been accessed.

[4] Data comparisons are made between data breach notifications from July 24, 2016 to July 23, 2017 (referred to as 2017 data breaches) and data breach notifications between the implementation of the data breach notification law and July 23, 2016 (referred to as 2016 data breaches).

[5] "2017 Cost of Data Breach Study," Ponemon Institute, June 2017.

[6] "2017 Cost of Data Breach Study," Ponemon Institute, June 2017.

[7] "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

[8] Tennesee code §§ 47-18-2107; 8-4-119.

Washington State Office of the Attorney General
1125 Washington St. SE
PO Box 40100
Olympia, WA 98504
(360) 753-6200
www.atg.wa.gov