2016 ATTORNEY GENERAL'S OFFICE DATA BREACH REPORT

Washington State Office of the Attorney General
September 2016

Report Contents:

- What is a data breach?.....p.2
- What are Washington state's data breach laws?.....p.3
- What information was compromised by data breaches?.....p.4
- How did data breaches in Washington happen?.....p.5
- How many Washingtonians were affected?.....p.6
- What industries were affected?.....p.7
- How do data breaches affect Washington businesses?.....p.8
- How does Washington compare with other states?.....p.10
- Resources for Businesses & Individuals.....p.11

Dear Washingtonians,

In response to several high profile data breaches that compromised the personal information of thousands of Washingtonians, in 2015 I requested legislation to update our data breach notification law. The bill was passed by the Legislature and took effect on July 24, 2015.

Under the updated law, consumers must be notified about data breaches as immediately as possible when their secured information, including encrypted and tokenized information, may be compromised. The notification must include sufficient information so that consumers can take steps to protect themselves from potential harm. Additionally, businesses are required to notify the Attorney General's Office when a data breach affects more than 500 Washingtonians. In the first year since these changes took effect, the Washington Attorney General's Office received 39 required data breach notifications.

Over the past year, data breaches affected Washington businesses such as hotel chains, telecommunications companies, a school district, a shipping company, retail stores, and tax preparation companies. In many cases, the breaches were the result of a targeted cyberattack, but in some cases, information was mistakenly lost or disclosed. Several companies experienced thefts of laptops, which may have contained compromised information. In another instance, a device containing personal information was lost aboard a ship, possibly on rough seas. The different circumstances of each breach show that data breaches can be hard to prevent, and how important it is that consumers are notified when their information may be compromised.

This report presents a snapshot of the data breach notices the Attorney General's Office received over the past year. As Attorney General, protecting consumers from identity theft and other threats is one of my top priorities. Tips and resources you can use if you experience identity theft are included at the end of this report. I hope you find this information helpful.

Sincerely,
Bob Ferguson
Washington State Attorney General

What is a data breach?

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. Data breaches are costly for the economy and can lead to individuals becoming victims of identity theft.

A data breach can occur by:

- **A malicious cyber attack, such as when a hacker electronically accesses and acquires computerized data;**
- **Unauthorized access, such as when an employee gains access to information that is not necessary for their job;**
- **Unintentional loss or theft, such as a briefcase or laptop computer containing client files that are stolen or misplaced.**

Executive Summary

- Data breaches reported to the Attorney General[1] compromised the personal information of over 450,000 Washington residents in the past year.
- Most data breaches affected less than 10,000 consumers.
- Financial account information was the most frequently compromised type of information.
- Malicious cyber attacks were the most common cause of data breaches affecting Washington residents.
- Data breaches impacted a wide segment of industries last year.
- The telecommunications industry experienced one reported breach last year, but this breach affected more Washington residents than all other breaches combined.

This report discusses only those data breaches that the Attorney General was notified about under Washington's notification law. Notices of breaches affecting fewer than 500 Washingtonians or compromising information not covered by Washington's notification statute were not included in the data compiled here.

What are Washington's data breach laws?

Notification

Businesses and public agencies are required to notify affected individuals when data breaches occur. At the request of the Attorney General, the Legislature updated Washington law in 2015 to reflect changes in technology.

Under the revised law, notification is required when a business or public agency experiences a breach of personal information if:

- The breach is reasonably likely to subject an individual to a risk of harm;
- The information accessed during a breach was not secured; or
- The confidential process, encryption key, or other means to decipher the secured information was acquired.

The notification laws, RCW 19.255.010 and RCW 42.56.590, cover "personal information." Personal information means someone's first name or first initial and last name in combination with any of the following:

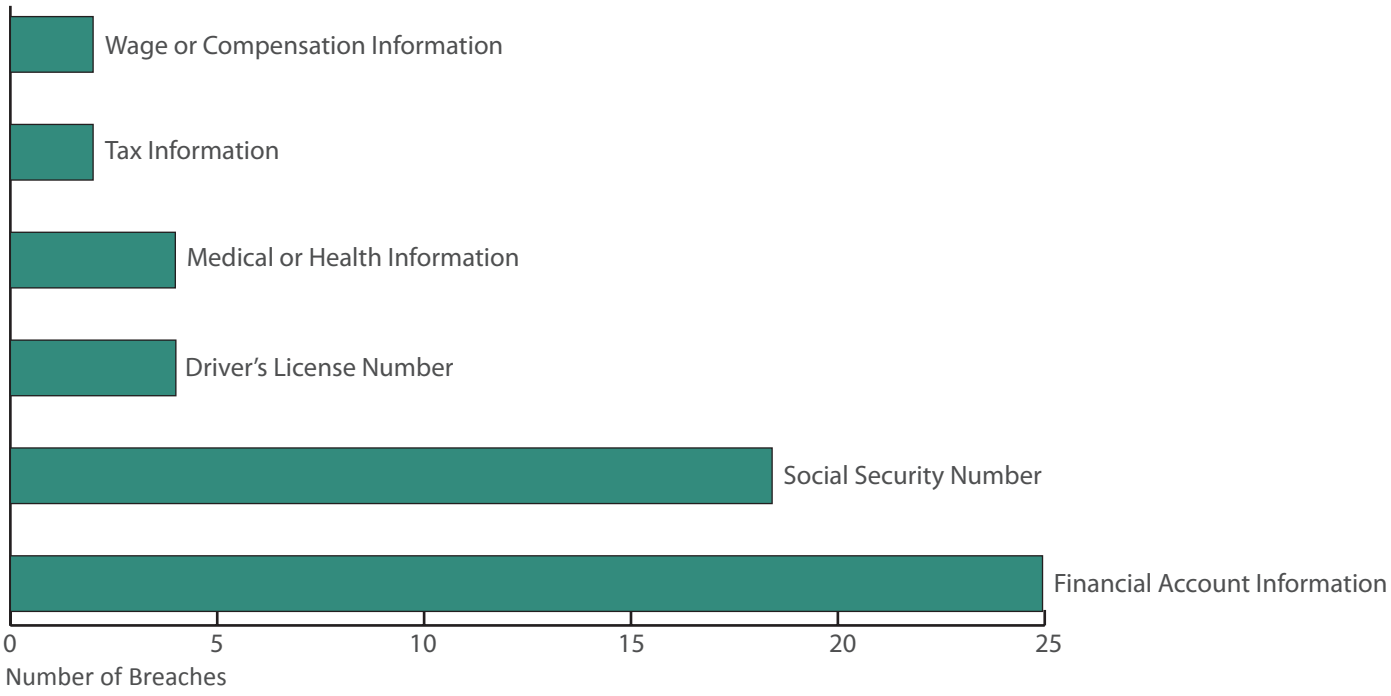
- Social Security number;
- Driver's license number or Washington identification card number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's account.

Theft of Financial Information

Washington's criminal law classifies improperly obtaining financial information as a Class C felony. Under this law, 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 as a Class B or C felony depending on the damage caused by the theft. Under Washington law, the crime of identity theft is focused on financial information.

What information was compromised by data breaches?

The types of information compromised by data breaches affecting Washington residents over the past year are noted in the graph below.

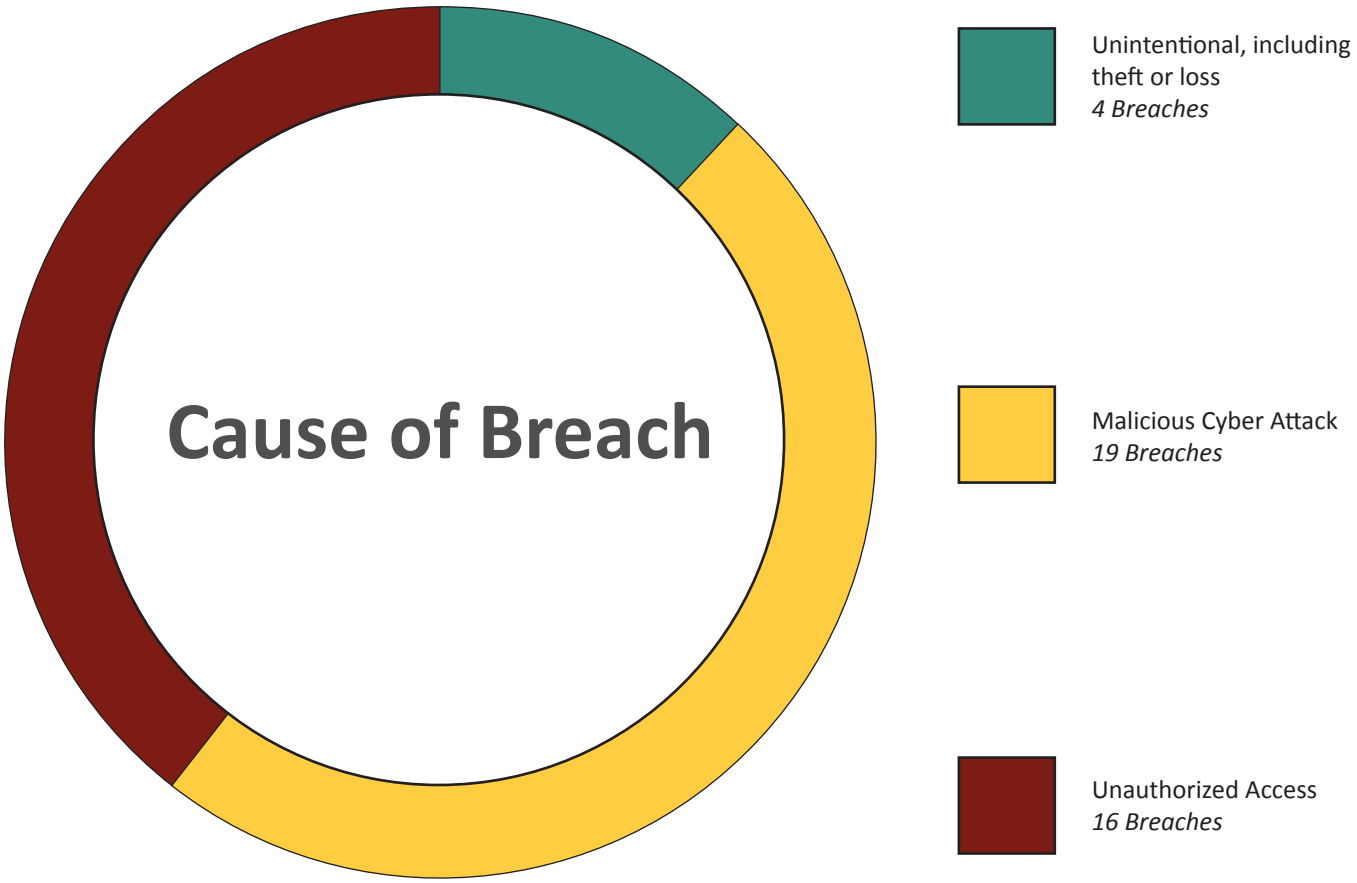


How do data breaches happen?

Malicious Cyber Attack
These are attacks where a third party attempts to gain access to secure data on a computerized network, website or other location. This can happen through the use of a virus or malware, impersonation of an employee, or another means of attack.

Unintentional Breach
This can include the loss or theft of information, including something as simple as the loss of a memory device or mail containing personal information sent to an out-of-date address. While these breaches are not caused by malicious intent, like all data breaches they have the potential to result in identity theft.

Unauthorized Access
This occurs when someone, who is not authorized, obtains access to information. This has happened when third-party vendors acquire access to a business's website or database, or when an employee is mistakenly allowed access to information when they shouldn't be.

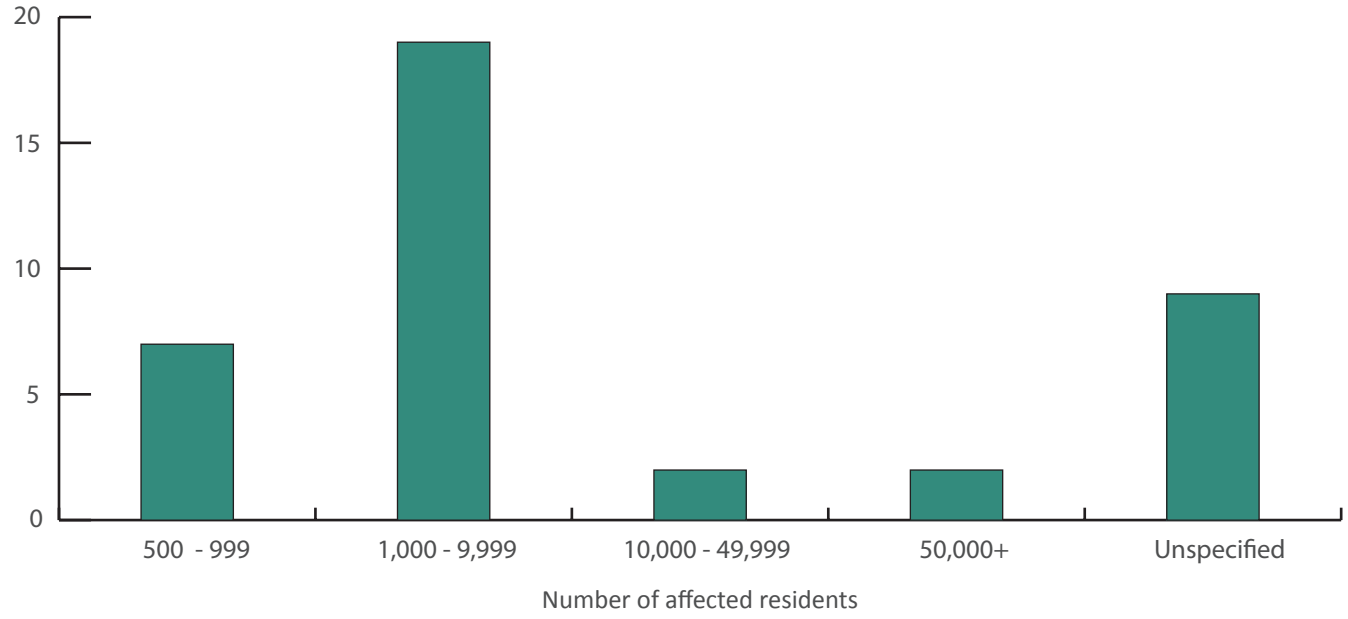


How many Washingtonians were affected?

Over the past year, breaches reported to the Attorney General's Office affected more than 450,000 Washington residents. Some individuals were likely affected by more than one breach. Several notifications were provided for breaches that affected an unknown number of people. The graph below shows the number of breaches affecting groups of different sizes. The most common breaches, by far, affected several thousand people.

Data breaches can compromise not only consumer information, such as when payment card information is hacked at a retail store, but can also compromise employee information at workplaces. At least three of the breaches in Washington over the past year specifically involved employee information. Any place where individuals share or use personal information can experience a data breach.

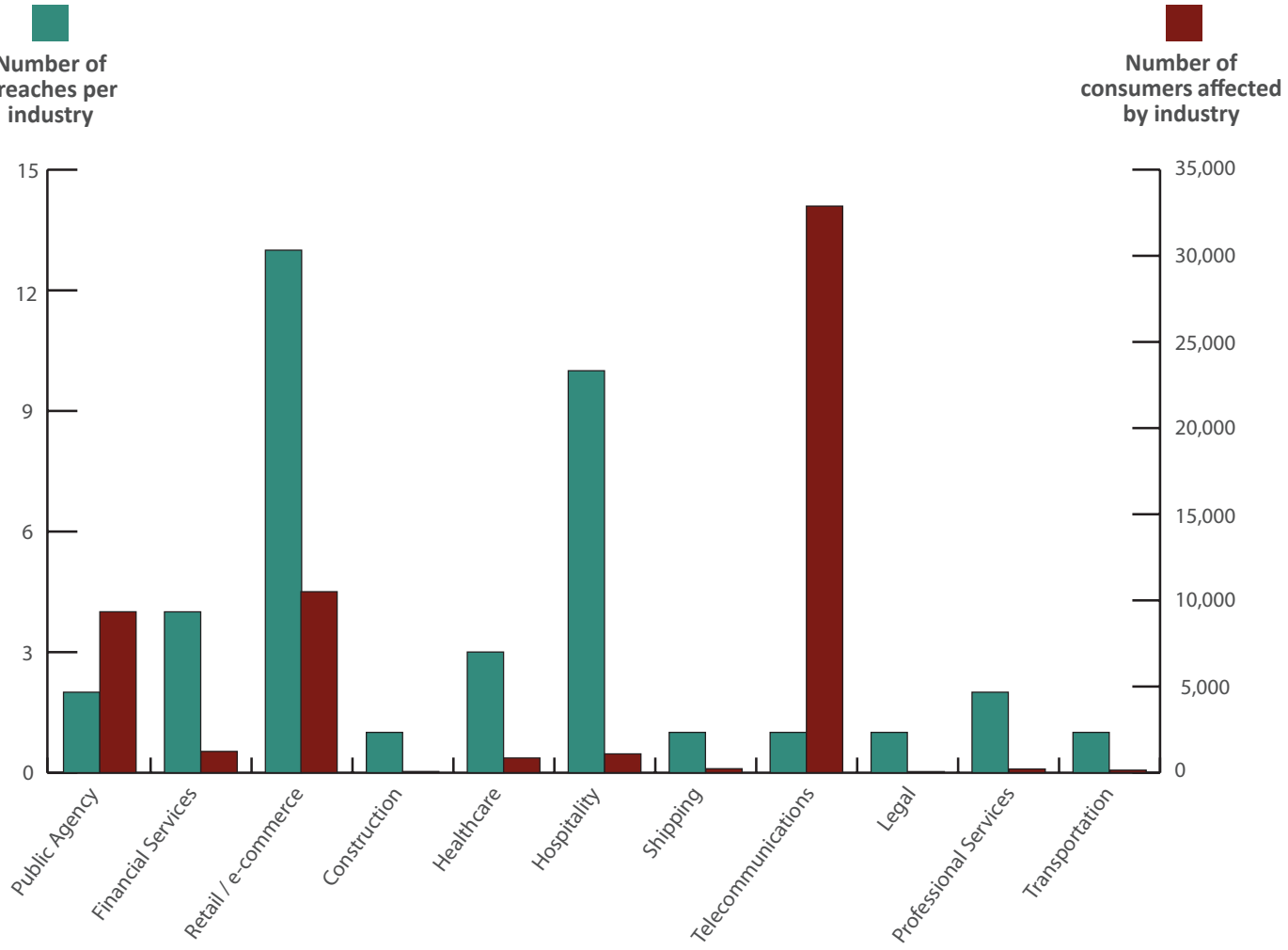
Number of reported data breaches by number of Washington residents affected



What industries were affected?

Data breaches affect nearly every industry. Any business is at risk for unintentional disclosures, such as the theft of a briefcase or a laptop or honest mistake by an employee. Thieves seeking personal information can be searching for more than just credit card or financial account information, resulting in a broad range of industries being targeted by cyber attacks.

The industries that had the most reported breaches affecting Washingtonians over the past 12 months were financial services, retail, health care, and hospitality. The telecommunications industry had only one breach, but that single breach affected the personal data of more than twice the number of Washingtonians affected by all other breaches, as shown in the graph below.



How do data breaches affect Washington businesses?

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 cyber attacks of all types, puts 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 and health care providers, construction companies, hotel chains and individual hotels, and small tax preparers.

A list of the breach notifications received by the Attorney General's Office can be found at: http://www.atg.wa.gov/data-breach-notifications.

Costs to Businesses

According to a study by the Ponemon Institute of the cost of data breaches in the United States, the average cost of a data breach to a business is $221 per compromised record.[1] Using this figure, data breaches likely cost businesses operating in Washington almost $100 million over the past year. The study found that $145 of this relates to indirect costs, such as turnover of customers resulting from the breach, and $76 are directly related to the breach, including legal fees, credit monitoring services for consumers, and security improvements.

As demonstrated by 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 notes: "It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs."[2] The study found that incident response plans and teams in place, extensive use of encryption to protect data, and employee training reduced the cost of a breach to a business. Third-party error, the cause of a number of Washington data breaches, increased the cost of a breach for a business.

1- "Cost of Data Breach Study in the United States" Ponemon Institute, June 2016, http://www-03.ibm.com/security/data-breach/

2 - P. 23.

Costs to Individuals

The U.S. Department of Justice's Bureau of Justice Statistics found in its "Victims of Identity Theft, 2014" study that 15 percent of people age 16 or older have experienced one or more incidents of identity theft in their lifetimes.[3] During the twelve month period of the study, seven percent of all U.S. residents were victims of one or more incidents of identity theft. In 2015, more than 9,000 Washingtonians filed complaints about identity theft with the Federal Trade Commission (FTC), although the actual number of identity theft victims is likely much higher.

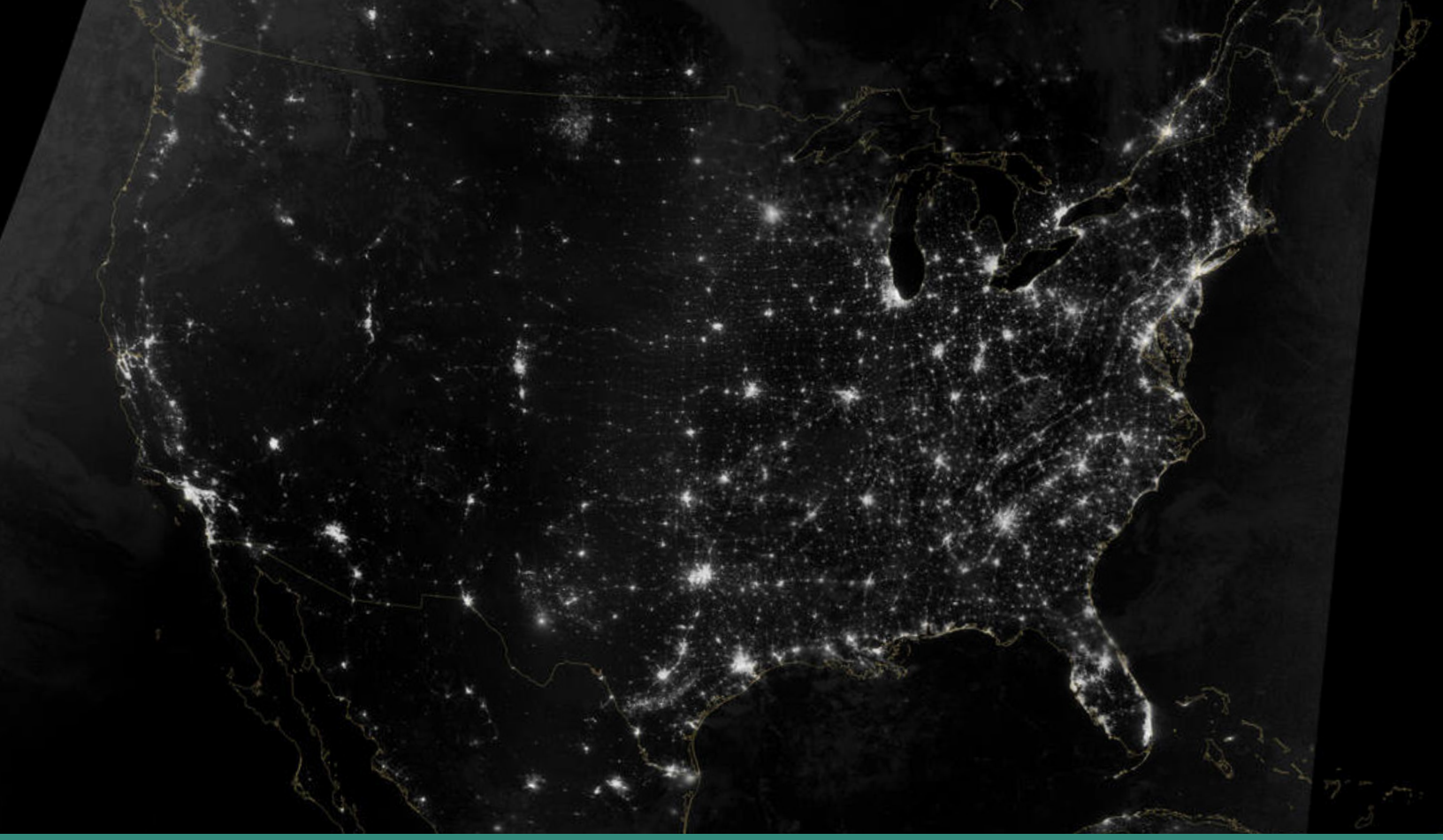
These instances of identity theft in the "Victims of Identity Theft report" include the fraudulent use of existing account information, such as credit card or bank account information, which was by far the most common type of identity theft. About 1 in 5 victims was affected by more than one instance of identity theft.

Not all victims of identity theft experience financial loss. The Department of Justice reports that nearly one-third of victims did not incur a direct financial loss. The type of information that is compromised affects the potential for financial loss. The cost to an individual can include financial loss from an account that is compromised, time spent securing personal information or closing accounts, and legal fees. In certain circumstances, a credit card or insurance company may reimburse part or all of the out-of-pocket financial loss.

Identity theft as a result of a data breach

Criminals attempt to steal sensitive personal information because they can use it or sell it. The damage that a thief can cause depends on the type of information acquired. Information can include name, address, phone number, email address, website account information (username and password), banking or financial information such as account number or payment card number, expiration date and security code, Social Security number, government identification number (most commonly driver's license number), and patient health information, such as insurance information or diagnoses.

3 - Bureau of Justice Statistics, "Victims of Identity Theft, 2014," Erika Harrell, Ph.D., September 27, 2015. http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408



How does Washington compare with other states?

Since 2005, almost all states have passed laws requiring businesses to notify consumers when a data breach occurs that may have compromised their personal information. Many of these laws have been updated since they were first enacted. There are differences in each state's requirements, particularly with respect to the way personal information is defined.

The differences in each state's notification laws make comparisons among the states difficult. For example, California law defines personal information more broadly than Washington does. As a result, the number of Californians reported as being affected by breaches is much higher, adjusted for population, than the number of Washingtonians reported as being affected by breaches.

Nationally, in 2015, the Identity Theft Resource Center is aware of 781 breaches that exposed at least 177,866,236 records, involving the theft of:

- Social Security numbers
- Credit or Debit Card numbers
- Email/Password/User names
- Protected Health Information

In a significant number of these breaches, the number of records compromised is unknown, which means that the number of total records exposed could be far higher.

4- http://www.idtheftcenter.org/Data-Breaches/2015databreaches.html

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 Attorney General's Office website at: http://www.atg.wa.gov/GUARDIT.ASPX

IdentityTheft.gov, provided by the U.S. Federal Trade Commission, is also a valuable resource for victims of identity theft.

Tips for dealing with identity theft:

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

Resources for businesses to protect themselves

The Attorney General's Office provides several resources for businesses to protect themselves from data breaches and to help explain the Washington 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, examining whether you need the information, and knowing what information you retain and how the information is retained.
2. Minimize the amount of information that you collect and retain. Delete unnecessary information.
3. Create and implement an information security plan.

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

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)