CHAPTER 9

# State Laws Protecting Citizen Information and Breach Notification Laws

IN THE UNITED STATES, there is currently no single comprehensive federal data privacy or security law. Instead, the United States has enacted industry-specific laws about security and privacy. These laws limit the use of personal information based on the nature of the data.

State governments also have entered this regulatory arena. States create data protection laws that are data specific. Many states have created laws to protect health and financial information. They also might try to protect data in certain types of records, such as motor vehicle records. In some ways, states are more aggressive in trying to protect personal information than the federal government.

This chapter focuses on state data protection laws. It includes laws from different states to give you an overview of the types of laws being passed to protect data. As you encounter issues regarding the law, security, and privacy, you must consider the impact of state laws and rules.

## Chapter 9 Topics

This chapter covers the following topics and concepts:

- What the history is of state actions to protect personal information
- What state breach notification laws are
- What state data-specific security and privacy regulations are
- What encryption regulations are
- What data-disposal regulations are
- What some case studies and examples are

## Chapter 9 Goals

When you complete this chapter, you will be able to:

- Describe state approaches to protecting the security of personal information
- Describe laws that protect certain types of data
- Describe state breach notification laws
- Describe the differences between state breach notification laws

# History of State Actions to Protect Personal Information

States have created many laws to protect personal information. California has worked hard to make laws that protect the security and privacy of its residents' data. It was this state's breach notification laws and a breach at a large corporation that led to the growth of data protection laws in many states.

## ChoicePoint Data Breach

ChoicePoint was a data broker. It merged public records, credit reports, and demographic data to create individual consumer profiles. It sold these profiles to the government and private companies. People used the profiles to conduct background checks. ChoicePoint also sold profiles to insurance companies. It collected many different types of personal information. It had names, addresses, and Social Security numbers. Its databases also included credit history and DNA information.

In February 2005, ChoicePoint notified 35,000 California residents that their personal data had been exposed in a data breach. California was the only state at that time with a **breach notification law.** The law applied to any business that stored the personal data of California residents. The law required them to notify state residents of any security breach involving their unencrypted personal information.

ChoicePoint said that it discovered the breach in late 2004. Law enforcement officials contacted the company about an identity theft ring. ChoicePoint learned that the criminals pretended to be its customers. In order to become a ChoicePoint customer, applicants had to provide proof of a lawful reason for buying consumer data. At the time of the breach, ChoicePoint had over 50,000 customers. They ranged from insurance companies to debt collectors.

> **NOTE**
>
> At the time of the data breach, news media reported that ChoicePoint had collected over 9 billion public records on U.S. residents. They reported that it had stored 250 terabytes of data.

ChoicePoint's validation processes didn't find the fake customers. Some of them provided suspect documents to ChoicePoint. For example, multiple businesses submitted documents with the same information. This should have raised red flags for more review. ChoicePoint later found over 50 fake accounts. These accounts had access to ChoicePoint's databases.[1]

At first ChoicePoint notified only California residents affected by the breach. This is because it was the only state requiring such notification. Nineteen other states were outraged. The state attorneys general wrote a letter to ChoicePoint. They demanded that it alert all people affected by the breach. ChoicePoint later sent notification letters to over 160,000 people.[2]

In January 2006, the Federal Trade Commission (FTC) investigated ChoicePoint. It alleged that ChoicePoint violated consumer privacy rights. It also charged the company with violating federal laws. ChoicePoint settled with the FTC in December of that year. It paid $10 million in civil fines.[3]

> **NOTE**
> ChoicePoint reported that it had many external audits after the 2005 breach. It was audited 80 times in the 24 months after the breach.

ChoicePoint also agreed to pay $5 million to fund a consumer relief program. The program would pay people who were victims of identity theft due to the breach. The agreement with the FTC also required ChoicePoint to create an information security program. It's required to get independent audits every year until 2026. At the time, the ChoicePoint settlement was the largest in the FTC's history.

> **NOTE**
> ChoicePoint was purchased by LexisNexis in 2008. To help protect consumer information, LexisNexis will give you a copy of your consumer file. You can request only your own file. You must also provide proof of identity to get a copy of the file. To learn more about this service, you can visit *https://personalreports.lexisnexis.com/*.

In May 2007, ChoicePoint settled a multi-state lawsuit over the breach. Forty-three states entered the settlement agreement. As part of that agreement, ChoicePoint promised to improve its process for verifying customers. It also agreed to strengthen how it protects the data that it collects. ChoicePoint also agreed to pay $500,000 to the states involved in the lawsuit.[4]

ChoicePoint was on the FTC's radar again in 2009. This time it was due to a 2008 security incident. ChoicePoint had changed some internal security controls. The changed controls failed to alert it that someone had unauthorized access to its data. The wrongful access continued for about 30 days. During this time, the data of about 13,750 people may have been disclosed. The data included Social Security numbers.

The FTC alleged that the 2008 incident was a violation of the 2006 agreement. As a result, ChoicePoint agreed to additional security requirements. It agreed to strengthen its information security program again. It was also required to report to the FTC on its security efforts every two months until 2011.[5]

The ChoicePoint data breach is unique because it spurred the creation of data breach notification laws in many states. If it weren't for the California breach notification law, ChoicePoint might not have notified any consumers at all about the data breach. Other states realized that their residents might not be able to protect themselves from identity theft in similar situations without these laws. Thirty-five states considered breach notification laws in 2005. The ChoicePoint case is widely seen as the reason why other states have these laws.

You can read FTC documents about the ChoicePoint case at *http://www.ftc.gov/enforcement/cases-proceedings/052-3069/choicepoint-inc.*

> **NOTE**
>
> Illinois Governor Rod Blagojevich proposed the Personal Information Protection Act just days after the ChoicePoint breach went public. The ChoicePoint breach affected about 5,000 Illinois residents. The act is Illinois's breach notification law. It took effect January 1, 2006.

## Breach Notification Regulations

California was the first state to have a breach notification law. It required businesses to notify their customers if they suffered a data breach that disclosed personal data. Many states have modeled their own breach notification laws on the California law. This section discusses the California breach notification law. It also discusses the laws in other states.

### California Breach Notification Act

California's Database Security Breach Notification Act law went into effect on July 1, 2003. The California legislature created the law after a security breach at a state-operated data facility. The legislature recognized that identity theft was one of the fastest growing crimes in California. It stated that people must act quickly to limit the harm caused by identity theft. The purpose of the law was to give California residents timely information so that they can protect themselves.

> **NOTE**
>
> California's breach notification law is Senate Bill 1386. This bill created the law.

The law applies to anyone who owns or uses computerized data that contains the unencrypted personal information of a California resident.[6] It applies to:

- State agencies
- Nonprofit organizations
- Private organizations
- Businesses

It also can apply to businesses that aren't actually located in California. It covers any entity that stores the personal information of a California resident. Under the law, an entity must notify California residents of a breach of its computer systems. They must give notice if unauthorized individuals access and take the resident's unencrypted data.

**FYI**

Under California law, a security breach means unauthorized acquisition of [illegible]. It must "compromise the security, confidentiality, or integrity of personal information" by an entity." This definition is confusing from an information security perspective because it refers to security and separately to confidentiality and integrity. Confidentiality and integrity are part of the standard definition of security. This type of imprecise definition [illegible] mation security professionals and lawmakers must work together in creating laws that [illegible] information security.

The law defines personal information very broadly. It's information that allows a person to be identified. *Personal information* is a person's first name or first initial and last name. The person's name is combined with any of the following:

- Social Security number
- Driver's license number or California Identification Card number
- Account number, or credit or debit card number, along with any security code, access code, or password that would allow access to a person's account
- Medical information
- Health insurance information

**NOTE**

California amended the law in 2008. The changes included adding medical and health insurance information to the law. They were not included as part of the original law.

Under the law, personal information is unencrypted data. If any of the items [illegible]

**FYI**

Under California law, a security breach means unauthorized acquisition of computerized data. It must "compromise the security, confidentiality, or integrity of personal information" held by an entity.[7] This definition is confusing from an information security perspective because it refers to security and separately to confidentiality and integrity. Confidentiality and integrity are part of the standard definition of security. This type of imprecise definition is why information security professionals and lawmakers must work together in creating laws that impact information security.

The law defines personal information very broadly. It's information that allows a person to be identified. *Personal information* is a person's first name (or first initial) and last name. The person's name is combined with any of the following:

- Social Security number
- Driver's license number or California Identification Card number
- Account number, or credit or debit card number, along with any security code, access code, or password that would allow access to a person's account
- Medical information
- Health insurance information

**NOTE**

California amended the law in 2008. The changes included adding medical and health insurance information to the law. They were not included as part of the original law.

Under the law, personal information is unencrypted data. If any of the data is unencrypted, then all of the information is considered personal information. Information that's available to the public through government records isn't personal information. The law also states that a username or e-mail address, when combined with a password or answer to a security question, is also personal information if those elements could be used to access an online account.

The law requires entities to notify California residents whenever a security breach occurs. They must also notify residents if they reasonably believe that a breach has occurred. They must notify people as quickly as possible. Under the law, there are two reasons to delay notification. The first is to figure out the scope of the security breach. An entity must do this so that it can notify the right people.

The second reason to delay notification is if law enforcement requires it. Law enforcement can allow entities to delay notification to conduct a criminal investigation. The entity must make the required notification as soon as possible after it's determined that it won't hurt the investigation.

The law requires entities to give written notice to California residents. When the law was first written, an entity just had to notify California residents of the security breach. The law didn't require that the notice have certain elements. However, the law was amended in 2011 to state that a notice must:

- Be written in plain language
- Include the name and address of the entity making the notice
- Include a list of the personal information that was potentially compromised in the breach
- Include facts about the breach, such as the date that it began and the date when it was discovered, as well as whether notification was delayed and why
- Contact information for the major credit reporting agencies

The 2011 amendments to the law also require entities to report to the California Attorney General if more than 500 California residents are affected by a single breach incident.

Sometimes providing notice to a large number of people can be very expensive. The California law allows entities to use a different type of notice if the entity can prove that:

- The cost of giving written notice is greater than $250,000
- The number of people to be notified is greater than 500,000
- It doesn't have sufficient contact information

If an entity can prove one of these situations, it doesn't have to give individual written notices. Instead, it must do all of the following to provide "substitute notice":

- Notify affected people by e-mail if the entity has an e-mail address for the person
- Post notice of the security breach on its Web site (if it has one)
- Notify major statewide media outlets about the breach

The California law provides a safe harbor for entities that encrypt personal information. A **safe harbor** is a legal concept. It refers to specific actions someone can take to show a good-faith effort to stay within the law and avoid prosecution. Entities that properly encrypt the personal information that they own or maintain don't have to follow the notification requirements if they have a data breach.

Finally, the law gives California residents a limited private cause of action against entities who don't follow the law. Residents who are harmed when an entity doesn't follow the law can sue for damages.[8]

**NOTE**

One major drawback of the California law is that it doesn't define an acceptable level of encryption. Other states have defined what type of encryption is sufficient to use as a safe harbor in their breach notification laws.

**NOTE**

In the law, a plaintiff can generally recover only damages in the amount that he or she has actually lost because of harm or injury.

## Other Breach Notification Laws

After the ChoicePoint breach, many other states created breach notification laws. As of January 2014, 46 states, including the District of Columbia, have these laws.[9] Many of them are based on the California law. Even though most states used the California law as a model, there are some differences. They include:

- Activities that constitute a breach
- Entities covered by the law
- The time for notifying residents
- Requirements that a notification contain certain types of information
- Minimum requirements for encryption
- Civil or criminal penalties for failing to notify affected people

Additionally, unlike the California law, most other state laws typically don't allow a private cause of action for failure to give notification.

### Activities That Constitute a Breach

The California law applies to unauthorized acquisition of unencrypted personal information. If attackers access the data, that's enough to trigger the law's notification requirements. Some other states require a showing of harm before notification is required. This means that attackers must not only access the data, but do something with it. For instance, the attackers must steal, copy, or change the data before notification is required. In addition, some sort of harm must be anticipated as a result. Stealing data is an anticipated harm under these laws. You must review the definition of *breach* carefully in each law to see what triggers the notification requirements.

> **NOTE**
> Other states that employ some sort of harm standard include Hawaii, Massachusetts, and Virginia.

In Arizona, there's a two-part test to see if notification is required. First, a breach is an unauthorized acquisition of personal information. This means that data must actually be taken. Second, the acquisition must cause, or be likely to cause, substantial economic loss to a person.[10] The harm caused must be substantial and economic. The law doesn't define the term *substantial*. Notice isn't required if the acquisition isn't reasonably likely to cause this type of harm.[11]

Ohio law also requires more than unauthorized acquisition to trigger notification. Under Ohio law, there also must be reasonably believed to be a material risk of identity theft or other fraud to an Ohio resident.[12] The risk of harm can also be a future risk of harm. In this law, the material risk of identity theft is enough to require notification.

### Entities Covered by the Law

The California law applies to any entity that owns or uses the personal information of California residents. It includes businesses, nonprofit organizations, and government agencies. Not all states have laws this broad. Some states specifically exclude state agencies from notification requirements.

Georgia's notification law doesn't apply to state agencies. Instead, it applies to information brokers. *Information brokers* are entities that sell personal data to other entities. The law states that it doesn't cover government agencies.[13] If a government agency experiences a breach, it doesn't have to notify affected residents under this law.

The Maine notification law as it was originally created was similar to the Georgia law. It also applied only to information brokers. It excluded state agencies. It was amended about a year after it was first enacted in order to include state agencies.[14]

**NOTE**

Why might a government exclude itself from its breach notification laws? Should it? Some states do hold themselves responsible for security breaches.

#### Entities Excluded from Breach Notification Laws

Some states exclude some kinds of entities from their breach notification laws. They do this because these entities are already subject to other laws with specific data security requirements. Many of these other laws have security and privacy obligations that are stricter than the states' own laws. If the entities are following these other laws, then a security breach may be less likely. In some cases, state lawmakers determined that making entities follow both the state breach notification law and the other laws would be too hard. It might hurt businesses operating in the state.

Some states exempt financial institutions covered by the Gramm-Leach-Bliley Act (GLBA). GLBA requires these institutions to protect a customer's nonpublic financial information. They must use security safeguards. They also must follow privacy rules. Breaches may be less likely if an institution follows GLBA. Many states exempt these entities from notification laws. They include Connecticut, Indiana, and Minnesota.

Some states also exempt entities that are covered by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA covered entities must follow rules designed to protect personally identifiable health information. They must follow the HIPAA Privacy and Security rules. Recent amendments also impose breach notification rules on HIPAA covered entities. These rules may be even stricter than some state notification laws. States that exempt HIPAA covered entities from their laws include Arizona, Rhode Island, and Wisconsin.

> **NOTE**
>
> A business day is an official workday. Business days are the days of the week that include Monday through Friday. Saturday and Sunday are not business days. Public holidays also aren't business days.

> **TIP**
>
> Remember, the reason for notification is to let people protect themselves from identity theft. Any delay in notifying people should be as short as possible.

### Time for Notification

Under the general California breach notification law, entities must give notice in the most expedient time possible. They must do so without unreasonable delay. A majority of states follow the California approach. However, some states require that entities give notice within a certain period.

Ohio law requires that notification be given to state residents in the most expedient time possible. However, that law states that entities must give this notice no later than 45 days after the discovery of the breach.[15] Florida has a similar requirement.[16]

In Maine, an entity may delay notification if requested by law enforcement.[17] An entity can only delay notification to help a criminal investigation. An entity must give notice once law enforcement determines that the notification will not hurt the investigation. At that point, the entity must provide notice within seven days.[18]

### Contents of Notification

Some states require that entities give notice in a certain way. The California law originally had no specific rules, but was modified several years after it was first enacted. Many states follow the original California model. There's a growing trend, however, to specify the types of information that should be included in a notice. States do this to make sure that residents get enough information to protect themselves.

North Carolina law requires that notice be given in a "clear and conspicuous" form.[19] This means that it needs to be easily understandable. The notice also must:

- Describe the incident in general terms.
- Describe the type of personal information that was involved in the breach.
- Describe how the entity is going to protect the personal information from additional unauthorized access.
- Provide a telephone number for the entity, if one exists, that a person may call for more information.
- Advise the person being notified to review his or her account statements and get a free credit report.
- Provide the toll-free telephone numbers and addresses for the major consumer reporting agencies.
- Provide the contact information for the FTC and the North Carolina Attorney General's Office, along with a statement that these sources have additional information about preventing identity theft.

North Carolina also allows entities to notify residents by telephone. The law allows this only if the entity makes direct contact with the people whose data was accessed in the breach. Colorado law allows notice to be given in written and electronic form.[20] It also allows notice by telephone.

### Encryption Requirements

The California law provides an encryption safe harbor. Entities don't need to give notice of a breach if the personal information in their computer system was encrypted. California law doesn't specify the lowest level of encryption needed to use the safe harbor. It also doesn't reference any industry standards.

Most other states also provide an encryption safe harbor. Some states also specify the encryption standards required to take advantage of the safe harbor. For instance, Indiana provides an encryption safe harbor. Its law says that data is encrypted if it's changed by an algorithmic process. It must be changed into a form that is unreadable without the use of a confidential process or key.[21]

The Indiana law also addresses key management. For portable electronic devices, like laptop computers, the data must be protected by encryption and the encryption key can't be stored on the device. Indiana law also says that data is considered encrypted if it's secured by any other method that makes the data unreadable or unusable.

**TIP**

Remember, a safe harbor is an action someone can take to show a good-faith effort to stay within the law.

**NOTE**

Algorithms are mathematical computations used to solve a problem. They're used to encrypt data.

### Penalties for Failure to Notify

California law doesn't impose any civil or criminal penalties if an entity doesn't notify state residents of a security breach. Other states do have penalties. In Texas, for example, the state can assess a fine against an entity that doesn't notify affected people.[22] The law states that an entity can be fined at least $2,000 for a violation. The fine can't be larger than $50,000 for a single violation.

Other states have more complicated penalty structures. Under Florida law, an entity that doesn't provide notification within 45 days of a breach faces potentially large fines.[24] It faces a $1,000-per-day fine for every day that the entity fails to give notice after the 45-day limit. This penalty is in effect for the first 30 days after the 45-day mark. After that, the fine increases to $50,000 for each additional 30-day period that the entity fails to give notice. This extends up to 180 days (about six months) after the 45-day mark. If entities don't give notification within 225 days after a breach, the state may fine them up to $500,000. Figure 9-1 illustrates the Florida fine structure.

**NOTE**

In Indiana, the failure to give notice is a deceptive act. The state attorney general's office has the power to prosecute deceptive acts. The fine for each act can be up to $150,000.[23]

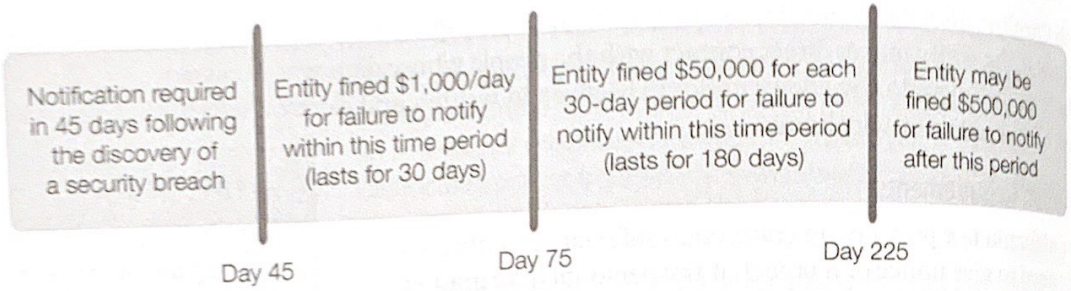


**FIGURE 9-1**
Florida fine structure for failure to give notification.

### Private Cause of Action

California law doesn't assess any penalties against an entity that doesn't follow the notification law. However, it does allow a person a private cause of action against those entities. People can sue the private entity for any damages they have because they didn't receive notification in a timely manner. Some states, such as Alaska, Maryland, and Alaska, allow a private cause of action; but some states don't. The states that don't are generally seeking to protect the entity's business. They also do this to protect the court system. It could be burdensome to the court system to process many individual cases. Instead, most of these states allow the state attorney general to pursue an action against the entity for failure to give notification. These states include Iowa, Michigan, and Oklahoma.

Almost every state now has a breach notification law to protect its residents. The laws have some similarities. Some laws also have unique requirements. These laws can be very confusing to businesses that operate in a number of states. Breaches at these entities are almost certainly going to affect people in many states. If this happens, an entity will have to review the laws of several states to properly notify people about the breach.

Breach notification is hard for entities because states have different laws about what constitutes a breach. An incident can be a breach in one state, but not another. It also can be hard if entities must give notice in a certain way or within a certain time. Differing penalties for noncompliance may also be a problem. Since the laws all have different nuances, it may not be enough for an entity to comply with the laws of its own state. Figure 9-2 provides a general decision tree that entities can follow in reviewing a security breach to see if notice is required.

The lack of uniformity among states may place additional burdens on businesses that experience a security breach. People also may be confused if they get notices that don't look similar. Notices might look different depending upon the law that the entity followed in creating the notice.

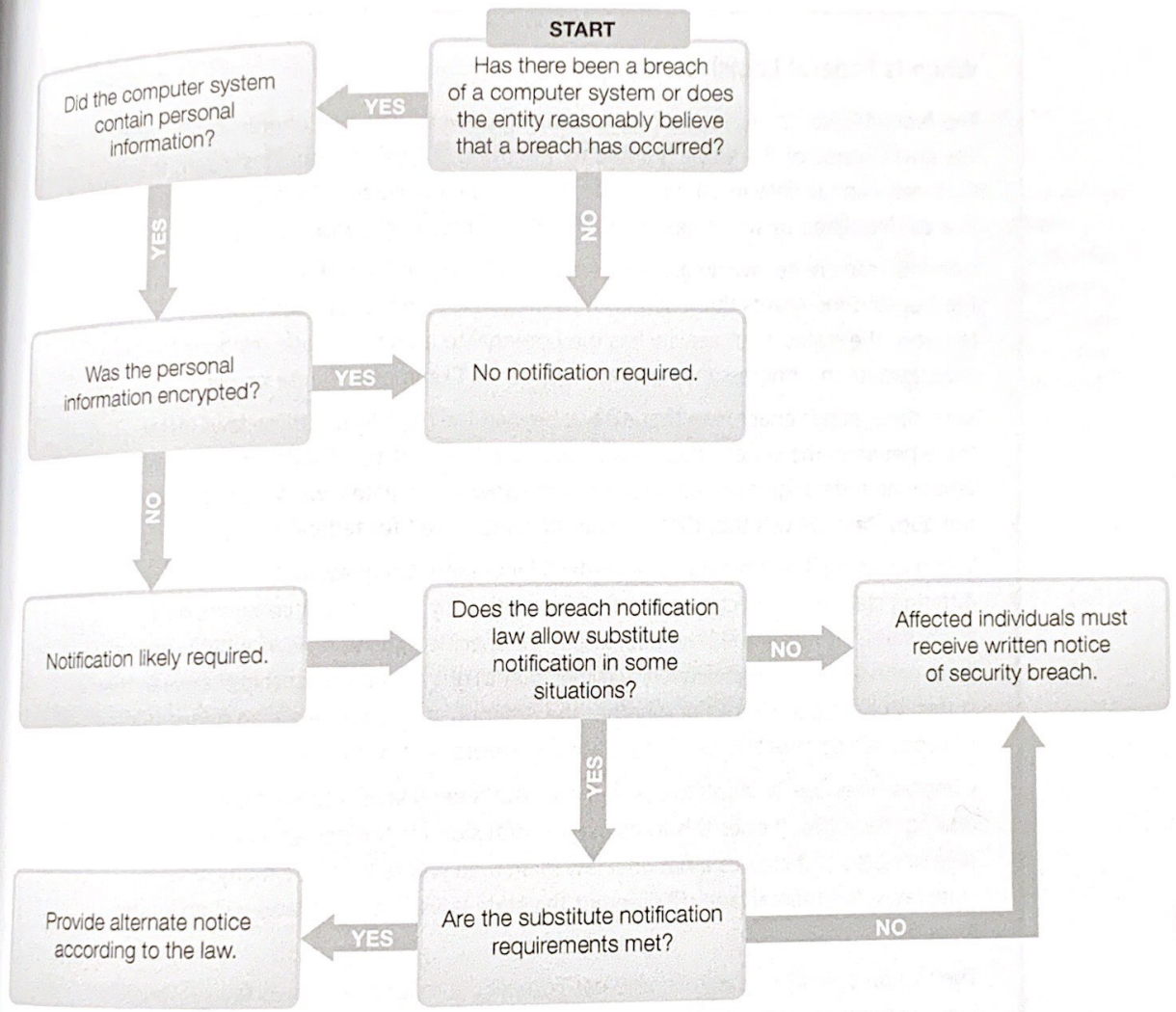


**FIGURE 9-2**
Breach notification decision tree.

In February 2014, the Obama administration recommended a federal breach notification law.[25] This recommendation was made in response to the Target Corporation credit card breach in late 2013. At least two acts were introduced in the U.S. Congress in 2014 that propose a uniform federal breach notification law. A federal breach notification law would create uniform requirements that any entity would have to follow to notify people of a security breach. A federal law would also likely make any state breach notification laws void. As of this writing, no act has yet passed Congress.

### When Is Federal Legislation Appropriate?

The federal government has limited lawmaking power. The U.S. Congress can't make any laws outside of the scope granted to it in the U.S. Constitution. This means that Congress can't usually interfere in state matters. It can't create a uniform federal law in areas legislated by the states unless there's a compelling reason to do so.

Congress can create laws in areas where the U.S. Constitution allows it. For instance, the Constitution grants the federal government the power to regulate commerce between the states. If an activity has the potential to affect the trade relations between the states, then Congress may address it under its Commerce Clause power.

Sometimes states enact laws that extend beyond their borders. If these laws affect trade between the states, then it's possible that they start to infringe upon an area where the federal government alone has the power to create laws. When this happens, the question rises whether that area has become "ripe" for federal legislation.

When deciding if an area is ripe for federal legislation, Congress looks at whether differing state laws affect activities that it traditionally regulates. It considers how many states have created laws addressing the specific topic. It reviews whether there's state confusion or complexity on activities that might affect relationships between the states. Congress also looks at whether the differing state laws create an undue burden or economic cost on businesses operating in several states.

Congress may use its legislative power to enact federal laws if there is confusion among the states. It does this to eliminate confusion for businesses that operate in several states. If it creates a national law in an area where there are many different state laws, the federal law will preempt the state laws. The state laws will no longer be valid.

The Congressional Research Service has compiled a report on various federal laws that may create breach notification requirements. The report notes that breach notification laws are complicated and often confusing. You can read the report at *http://www.fas.org/sgp/crs/misc/R42475.pdf*.

## Data-Specific Security and Privacy Regulations

Many states have created laws to protect the use of certain types of information. Like the federal government, they create laws by data type. This section discusses some of the data-specific laws that states have created to protect personal information.

## Minnesota and Nevada: Requiring Businesses to Comply with Payment Card Industry Standards

Some states have started to create laws that require entities in the state to comply with industry security standards. Minnesota and Nevada have created laws that require businesses operating in those states to comply with parts of the Payment Card Industry (PCI) Data Security Standard (DSS).

Minnesota created the first state law that attempted to codify certain parts of the PCI DSS. This law is called the Plastic Card Security Act. It was effective August 2007. It forbids businesses from storing cardholder information for more than 48 hours after the credit card transaction is approved.[26] Information that can't be stored includes:

- Card verification number
- PIN number
- Contents of the card magnetic stripe

**NOTE**

Businesses that wish to accept credit cards for payment must follow the PCI DSS. The major credit card companies require it. It isn't a law. Credit card companies like Visa and MasterCard enforce PCI DSS.

The PCI DSS also states that businesses may not retain this information. The Minnesota law has turned this part of the PCI DSS industry standard into a law.

The Minnesota law shifts the cost of a breach to a business that violates the law. If a business suffers a breach, and is found to have violated the storage requirements, then it can be held responsible for costs related to the breach. For instance, a bank or other financial institutions can sue the business to recover their costs in responding to the breach. These costs include issuing new cards or refunding unauthorized charges.[27]

### The Minnesota Plastic Card Security Act Supported by Financial Institutions

One of the reasons the Minnesota Plastic Card Security Act was introduced was the 2007 TJX data breach. Financial institutions often paid the cost for notifying people that their credit and debit card information was disclosed in a breach. There were other costs as well. If another organization suffered a breach that included card data, financial institutions had to reissue the cards to their customers. Reissuing the cards cost money. They had to refund unauthorized changes. They also suffered reputation damage when customers asked whether the financial institution was also involved in the breach.

The Minnesota Credit Union Network was tired of paying for another organization's weak security practices. The network is an association of more than 160 credit unions in Minnesota. It engages in political advocacy, education, and awareness activities. It pushed for the creation of the Plastic Card Security Act. It wanted this law to help reduce its costs for another organization's security breach.

> **NOTE**
> The Nevada law states that "personal information" is a person's name combined with Social Security number, financial account number, and driver's license or other identification number.[29]

Nevada is the first state to make following the entire PCI DSS a state law requirement. In 2009, the Nevada legislature modified the state's Security of Personal Information Law. The law had been in effect since 2005. The law requires protection of personal information in a number of ways. The 2009 changes to the law added PCI DSS language. These changes were proposed in Nevada Senate Bill 227.[28] The law now requires businesses to follow the PCI DSS. It went into effect January 1, 2010.

The Nevada law applies to "data collectors."[30] Data collectors are:

- State agencies
- Financial institutions
- Businesses that handle personal information

The law requires any data collector who accepts credit cards for the sale of goods or services to comply with the current version of PCI DSS. It also states that a data collector isn't liable for damages from a data breach if it complies with the law. Entities that comply with the law will likely not expose credit card information in a security breach. The only exception to the law's safe harbor is if the data collector's own gross negligence caused the breach.

The Nevada law is novel because it's the first time that following the entire PCI DSS is required by law. Some commentators think that the new Nevada law will encourage other states to adopt similar laws. Others believe that the law is problematic. This is because businesses that accept credit cards already have to comply with the PCI DSS under their contracts with credit card companies. If they violate the PCI DSS, they can be subject to large fines from those companies. These commentators believe that the Nevada law's safe harbor terms may be confusing to businesses that accept credit cards. This is because the law will not protect them from fines from the credit card companies.

## Indiana: Limiting SSN Use and Disclosure

> **NOTE**
> The Social Security Administration created the Social Security number in 1936. It created the SSN to track worker earnings. This was necessary to administer the Social Security program.

Some states have created laws protecting Social Security numbers (SSN). These laws recognize that SSNs are highly sensitive pieces of information. An SSN can be very valuable to an identity thief. Thieves can use the number to easily establish new identities to commit identity theft crimes.

Indiana has laws designed to protect SSNs. Its laws forbid SSNs from appearing in public documents. It also has laws that forbid state agencies from disclosing a person's SSN to any other person or entity.

### The Importance of Legislative History

All laws have a **legislative history**. This history documents the number of times that a law is modified during the period from introduction to signing. It includes any materials generated in the course of creating legislation. It includes committee reports and hearings. It also includes transcripts of debate and reports issued by legislatures. The legislative history can be reviewed to help determine what a legislature intended when it created a law. The Nevada law requiring data collectors to follow PCI DSS went through many changes. You can read the law's legislative history at *http://www.leg.state.nv.us/Session/75th2009/Reports/history.cfm?DocumentType=2&BillNo=227*.

When Senate Bill 227 was first introduced, it contained no language requiring data collectors to follow PCI DSS. Instead, it required data collectors to use certain types of approved encryption technologies. After the bill was introduced, industry groups contacted the bill's author. They expressed concerns about the bill. They opposed it because it was not technology neutral. You can read the letter submitted by industry groups at *http://www.leg.state.nv.us/75th2009/Exhibits/Assembly/CMC/ACMC1140C.pdf*.

After negotiation, the bill was amended to include the PCI language. Little information was included in the legislative history to indicate why the PCI language was added. A question that remains is whether the businesses that objected to the bill's original language are happy with the final law that requires PCI compliance.

Since 2006, Indiana law has stated that county recorders' offices may not accept any document for recording that contains an SSN.[31] The only time that they can accept a document containing an SSN is when another law requires that the document contain an SSN. Some types of federal laws, such as releases of federal tax liens, require the use of an SSN.

The state also was concerned that public records recorded before 2006 could contain SSNs. Identity thieves could use these documents to get SSNs. Since 2008, Indiana law states that county recorders can't provide a recorded document to a member of the public unless they first search the document for SSNs. If they find a document with an SSN, they

**FYI**

A county recorder's office keeps public records about certain types of transactions. These offices usually handle legal documents regarding real estate ownership. These documents are filed, or *recorded*, with a county recorder's office. This is done to give public notice of the transaction. Certain types of records also can be filed with a county recorder for future reference or safekeeping.

must redact it before allowing public inspection. It's a civil violation for a county recorder or any employee to disclose a recorded document containing an SSN without first searching the document for an SSN. The law doesn't cover disclosure of the last four digits of an SSN.

Other states have laws designed to protect SSNs. Arizona law prohibits printing an SSN on government or private identification cards. This law also prohibits the transmission of a person's SSN over an unsecured Internet connection.[32] California law forbids companies from requiring people to transmit an SSN over the Internet unless the connection is secure or the SSN is encrypted.[33]

Indiana law also provides that a state agency may not disclose a person's SSN to anyone.[34] This law went into effect on July 1, 2006. State agencies include an elected official's office and state educational institutions.

There are limited exceptions to this law. A state agency is allowed to disclose an SSN if:

- A person gives explicit written consent for the disclosure of their SSN
- The disclosure is required by state or federal law
- The disclosure is required by a court order

> **NOTE**
>
> One of the biggest differences between civil law and criminal law is punishment. In civil law, a defendant isn't sent to jail as a punishment. Instead, civil law imposes fines. Civil law also requires a defendant to reimburse a plaintiff for damages. In criminal law, punishment usually involves fines or prison sentences, or both.

The law lists very specific penalties for an inappropriate disclosure of a person's SSN. The state agency is not responsible for these penalties. Instead, they are directed at the state agency employee who disclosed the SSN. For instance, a state agency employee who "knowingly, intentionally, or recklessly" discloses an SSN in violation of the law commits a Level 6 felony. This is a criminal sanction. In Indiana, a Level 6 felony can result in a prison term between six months and three years. In addition, a person can be fined up to $10,000.[35]

If a state agency employee negligently discloses an SSN, the person commits a Class A infraction. In Indiana, an infraction is a civil sanction. A person can't be imprisoned for an infraction. However, he or she can receive a fine of up to $10,000.

Under the law, if a state agency impermissibly discloses an SSN, it must notify the affected person. It also must notify the state attorney general's office. Under the law, the state attorney general has the authority to investigate an improper disclosure of an SSN. The state attorney general also can make additional rules to carry out the nondisclosure law. Individuals don't have a private cause of action under the law. They can't sue a state agency for wrongfully disclosing an SSN.

## Encryption Regulations

Some states require entities doing business within the state to follow basic information security practices. These practices protect the security and privacy of data. Other states are more aggressive. They require entities to use specific security practices, such as encryption.

**FYI**

The Massachusetts Office of Consumer Affairs and Business Regulation held a public hearing on the data protection standards in January 2009. The hearing showed that businesses were worried about meeting the standards. You can read a transcript from the hearing and written comments at *http://www.mass.gov/ocabr/docs/idtheft/201cmr17comments.pdf*.

## Massachusetts: Protecting Personal Information

Massachusetts has created some of the nation's most rigorous data protection laws. It created its breach notification law in 2007.[36] That law also required the state's consumer affairs department to issue standards for the protection of personal information. The law stated that the standards should:

- Protect the security and confidentiality of personal information consistent with industry standards.
- Protect against anticipated threats to the security or integrity of personal information.
- Protect against unauthorized access to or use of personal information that could harm a person.

The Massachusetts "Standards for the Protection of Personal Information of Residents of the Commonwealth" was released in September 2008. It originally was scheduled to take effect January 1, 2009. The state pushed back compliance to March 1, 2010. It did this in response to public comments on the regulation. The state released the final version of the standard in August 2009.[37]

Entities must follow the data protection standard to safeguard personal information. They must protect data in paper and electronic form. The standard has broad application. Any person that uses and stores personal information about Massachusetts residents as part of the sale of goods and services must comply with it. It also applies to anyone who keeps this type of information for employment purposes. It doesn't apply to state agencies.

The standard applies to personal information about Massachusetts residents. The definition is similar to the definitions used in breach notification laws. Those laws are discussed at the beginning of this chapter. Under the data protection standard, personal information is a person's first and last name, or first initial and last name, and any of the following:

- Social Security number
- Driver's license number or state identification card number
- Financial account number, or credit or debit card number, with or without password or PIN

> **NOTE**
> The Gramm-Leach-Bliley Act (GLBA) is a law that requires entities engaged in certain kinds of financial transactions to follow privacy and information security rules. These rules are designed to protect customers' personal information.

The standard requires entities to create an information security program. It states that an entity's information security program must be a good fit for its size and scope. It also must fit the entity's type of business. It must describe the administrative, technical, and physical controls that protect the personal information used by the entity. The program requirements are similar to those stated in the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule.

The standard uses a risk-based approach to information security. It allows the entity to review its resources and data use. It also can review its needs for security and confidentiality. The entity can use the results of this review to determine the safeguards it should use. As part of its program, an entity must:

- Assign an employee to manage the program
- Conduct a risk assessment to identify risks to the security, confidentiality, and integrity of information. Review current safeguards to make sure that they are effective
- Develop policies for use of personal information off business premises
- Develop disciplinary policies for failure to follow the information security program
- Develop policies to keep terminated employees from accessing personal information
- Select service providers and make sure that any contract includes terms to protect personal information
- Develop policies to physically safeguard personal information
- Monitor and review the program to make sure it's effective
- Document actions taken in response to any security breach[38]

> **NOTE**
> Under the standard, "technically feasible" means that if there's a reasonable way to accomplish a required technology result, then an entity must do so.

The standard also includes computer system security requirements. This part of the standard directs entities to implement the security requirements. They must do this as long as the requirements are technically feasible. An entity doesn't have to apply requirements that aren't technically feasible.[39]

The standard states that an information security program must include specific security requirements. They are:

- Secure user authentication
- Secure access control measures
- Encryption of all transmitted personal information that travels across public networks, and encryption of information to be transmitted wirelessly
- Reasonable monitoring of systems
- Encryption of all personal information stored on laptops or portable devices
- Up-to-date firewall protection and operating system security patches on computers containing personal information
- Virus and malware protection
- Security awareness and training activities

**FYI**

Massachusetts has released frequently asked questions (FAQs) about its data protection standard. You can read them at *http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf*.

The encryption requirements have received a lot of attention. They require businesses to encrypt the personal information of Massachusetts residents while it's stored on their systems. They also must encrypt it when it's transmitted. The standard doesn't define a preferred method of encryption. Encryption is defined in a technology-neutral way. Under the standard, encryption is changing data into an unreadable form. The encrypted data can't be read or understood without an encryption key. Encryption keys are used to encrypt and decrypt data.

The Massachusetts attorney general has the authority to enforce the data protection standard. The law allows civil penalties of up to $5,000 for each violation. The attorney general can also make an entity pay for the costs of an investigation into any violations. Entities can also be charged attorneys' fees.[41]

**NOTE**

While the data protection standards don't define a preferred method of encryption, the Massachusetts breach notification law does. Under the state's breach notification law, encryption is defined as a transformation of data through the use of a 128-bit or higher algorithmic process. The process must change into a form that is unreadable without the use of a key.[40]

The Massachusetts data protection standard is unique. It attempts to regulate businesses outside of Massachusetts by requiring businesses to encrypt the personal data of Massachusetts residents. This may be hard since businesses typically must follow only the laws of the state where they are located. Under the law, this is a jurisdiction issue. Only revisions to the standard, or a court case, will help clarify how widely the state may enforce this standard.

## Nevada Law: Standards-Based Encryption

Nevada law also has encryption requirements. Its law has had encryption rules since 2008. They were strengthened in 2009 as part of Nevada Senate Bill 227. This same bill required data collectors in the state to follow PCI DSS. The PCI DSS portion of the bill was discussed earlier in this chapter. Senate Bill 227 went into effect January 1, 2010.

The Nevada law requires data collectors to use encryption if they are transmitting personal information outside of their business network. They must encrypt the data if it's sent externally via e-mail or any other electronic transmission. This requirement helps protect data while it's being transferred from one entity to another. The Nevada law excludes facsimiles from the transmission encryption requirements.[42]

> **NOTE**
> Nevada law defines data storage devices as computers, cell phones, and external computer hard drives. It also includes backup storage media.

The law also requires data collectors to encrypt personal information on any data storage device that is moved beyond the technical or physical controls of their business. This means that they must encrypt any storage device that leaves the business location. They must encrypt backup tapes containing personal information that they send to an off-site storage facility. This portion of the law helps protect data if the storage media is lost or stolen.

The encryption rule is novel because of its breadth. It covers data when it's stored and when it's transmitted. The law is also interesting because of how it defines encryption. This is one area where the Nevada law varies greatly from the Massachusetts encryption law. The Massachusetts law defines encryption in a technology-neutral way. It doesn't reference any industry standards. The Nevada law, however, references industry standards.

> **NOTE**
> You can read the Federal Information Processing Standards at *http://csrc.nist.gov/publications/PubsFIPS.html*.

Under the law, data collectors must use encryption technologies adopted by a standards-setting body. The law references the Federal Information Processing Standards. These standards were issued by the National Institute of Standards and Technology (NIST). Under the law, the technology used must make the personal information unreadable.

The law also requires that data collectors use good cryptographic key management practices. These practices protect encryption keys. Encryption keys encrypt and decrypt data. They must be carefully guarded. These keys protect the confidentiality of data. They also protect the integrity of the whole encryption process. The law requires data collectors to use key management practices created by a standards setting body. Again, the law specifically refers to NIST standards.[43]

A data collector that complies with the law isn't liable for damages resulting from a security breach. This protection extends to a breach so long as the data collector's own gross negligence didn't cause the breach.

The Nevada law gives guidance to data collectors on what is considered an acceptable level of encryption. This helps bring clarity to the law. It also gives information security practitioners help in advising businesses on encryption strategies.

The law does create some other ambiguities. For instance, Nevada's breach notification law provides a safe harbor for the unauthorized access of personal information. If an entity encrypts this information, then notification isn't required. The breach notification law doesn't define encryption with the same detail as the encryption law. It's possible that the new law might become the default standard used to specify a minimum level of encryption. This standard could then be applied to entities seeking the breach notification law safe harbor. It isn't known if the Nevada legislature intended this.

## Data Disposal Regulations

As of January 2014, at least 30 states have created data disposal laws.[44] They have created these laws to make sure that personal information is properly disposed of. Personal data must be protected throughout its lifecycle. This includes disposing of the information in an appropriate way.

### Washington: Everyone Has an Obligation

Washington State created its personal data disposal law in 2002.[45] In creating the law, the state legislature made comments about how important the law was. It said that:

- Careless disposal of personal information causes a significant risk of identity theft
- Improper disposal threatens a person's privacy and financial security
- Everyone in the state has a duty to dispose properly of personal information[46]

> **NOTE**
>
> The only entity specifically excluded by the Washington law is the federal government. The law also states that entities that comply with the GLBA Safeguards Rule are considered compliant with the state law.

The Washington disposal law applies to any person or entity in the state. It requires an entity to take reasonable steps to destroy records that contain health and financial data when it determines that it no longer needs those records.

The law requires entities to properly destroy information held in their records. *Records* are defined as any material that holds information. It includes paper or electronic materials. Entities must make sure that they destroy any personal financial or health information in their records. Personal financial and health information is data that identifies a person and is commonly used for financial or health care reasons.

The law states that an entity must destroy information in records so that it's no longer readable or decipherable. The law states that proper destruction includes shredding, erasing, or modifying records so that they're no longer readable.[47]

The Washington law allows a person harmed by a violation of the law to sue the entity that violated it. The law provides the plaintiff with several remedies. The remedies vary depending on the type of violation. If the entity's failure to comply with the law was due to negligence, a court may award a penalty of $200 or actual damages. The court must award a plaintiff whichever amount is greater.

If an entity's failure to comply with the law was intentional, then the court can award a penalty of $600 or actual damages. Again, the court must award whichever amount is greater. The law also allows the court to award "treble" (triple) damages. Treble damages are three times the amount of the actual damages incurred. The law states that treble damages may not be more than $10,000.[48]

> **NOTE**
>
> *Treble damages* are damages that punish a defendant for intentional conduct.

The law also allows the state attorney general to prosecute an entity that violates the law. In that instance, a court must award damages the same way that it awards damages to an individual plaintiff. The court may also grant injunctive relief. This means that it can order the entity to stop violating the law.

## New York: Any Physical Record

On the other side of the country, New York State also has a data disposal law.[49] Its law states that no person or business may dispose of a record containing "personal identifying information" without shredding, destroying, or modifying it so that the information is no longer readable. The law requires that any person or business destroying the records must take action that is consistent with commonly accepted industry practices. They must use these practices to make sure that no unauthorized person has access to information in the record.

> **NOTE**
> The New York law specifically excludes state agencies.

Under the New York law, *records* are any information held in any physical form. They can be paper or electronic. They include reports, letters, and computer tapes. Any type of data storage medium is a record. Personal identifying information is information in a record that identifies a person by name and includes any of the following:

- Social Security number
- Driver's license number or identification card number
- Mother's maiden name, financial account numbers or code, or any other identification number

### Confidential Documents Used as Confetti

If you are a Yankees fan, 2009 was a very good year. It was their first World Series win since 2000. They celebrated their 27th World Series win with a ticker tape parade in New York City on November 4, 2009.

The term "ticker tape parade" originated in New York City. These parades are rare now; real ticker tape hasn't been used since the 1960s. They are traditionally reserved for large celebrations, such as sports victories.

The 2009 parade for the Yankees was the first ticker tape parade in New York City since the Giants won the Super Bowl in 2008. Sports fans were very excited. When they ran out of confetti, they dumped any type of paper that they could find from skyscraper windows. This included documents containing personal information. News media reported that after the parade, law firm memos, banking records, and court files were recovered from the debris in the street.

One financial firm had to discipline an employee who threw documents marked for destruction instead of confetti. The documents contained financial information and Social Security numbers.