



# The Definitive Guide to U.S. State Data Breach Laws

# The Definitive Guide to U.S. State Data Breach Laws

According to the [National Conference of State Legislatures](#) (NCSL), legislation has been enacted by all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands that requires private entities or government agencies to notify individuals who have been impacted by security breaches that may compromise their personally identifiable information.

These laws typically define what is classified as personally identifiable information in each state, entities required to comply, what specifically constitutes a breach, the timing and method of notice required to individuals and regulatory agencies, and consumer credit reporting agencies, and any exemptions that apply, such as exemptions for encrypted data.

Entities that conduct business in any state must be familiar with not only federal regulations, but also individual state laws that apply to any agency or entity that collects, stores, or processes data pertaining to residents in that state. While the laws in many states share some core similarities, state legislators have worked to pass laws that best protect the interests of consumers in their respective states. As a result, some states have much more stringent laws or more severe penalties for violations. Below, you'll find a state-by-state guide providing a detailed synopsis of the state's existing data breach laws, notification requirements, penalties for violations, and pending legislation.

- [Alabama](#)
- [Alaska](#)
- [Arizona](#)
- [Arkansas](#)
- [California](#)
- [Colorado](#)
- [Connecticut](#)
- [Delaware](#)
- [Florida](#)
- [Georgia](#)
- [Hawaii](#)
- [Idaho](#)
- [Illinois](#)
- [Indiana](#)
- [Iowa](#)
- [Kansas](#)
- [Kentucky](#)
- [Louisiana](#)
- [Maine](#)
- [Maryland](#)
- [Massachusetts](#)
- [Michigan](#)
- [Minnesota](#)
- [Mississippi](#)
- [Missouri](#)
- [Montana](#)
- [Nebraska](#)
- [Nevada](#)
- [New Hampshire](#)
- [New Jersey](#)
- [New Mexico](#)
- [New York](#)
- [North Carolina](#)
- [North Dakota](#)
- [Ohio](#)
- [Oklahoma](#)
- [Oregon](#)
- [Pennsylvania](#)
- [Rhode Island](#)
- [South Carolina](#)
- [South Dakota](#)
- [Tennessee](#)
- [Texas](#)
- [Utah](#)
- [Vermont](#)
- [Virginia](#)
- [Washington](#)
- [West Virginia](#)
- [Wisconsin](#)
- [Wyoming](#)
- [District of Columbia \(Washington, D.C.\)](#)
- [Guam](#)
- [Puerto Rico](#)
- [Virgin Islands](#)

## Alabama

**Reference:** [S.B. 318](#)

**Summary:** Alabama became the final state in the U.S. to enact a data breach notification law on March 28, 2018. Named the [Alabama Data Breach Notification Act of 2018 \(S.B. 318\)](#), it went into effect on June 1, 2018. Alabama required both Covered Entities and Third-Party Agents to notify affected individuals of a data breach when the breach is deemed likely to cause substantial harm to the individuals impacted. Alabama's Data Breach Notification Act also includes a provision that requires the disposal of data through shredding, erasing, or otherwise modifying sensitive information when that information is no longer required to be retained per applicable laws, business regulations, or business needs. The law does not apply to covered entities that are subject to other federal or state laws, regulations, procedures, or guidance on data breach notifications provided that the covered entity maintains the proper procedures under those laws or regulations, provides acceptable notice to affected individuals in the event of a breach, and provides a copy of the notice to the Alabama Office of the Attorney General in a timely manner when the entity notifies 1,000 or more individuals.

Covered entities and third-party agents are required to maintain reasonable security measures to protect personally identifying information, including the designation of an employee to coordinate these security measures, methods and processes for identifying the risks of a security breach, both internal and external, evaluation and adjustment of security measures to adapt to changes in circumstances that may impact the security of sensitive information, and other measures.

### **Notification Requirements:**

Notification is required if, following a prompt and thorough investigation, it is deemed that the security breach is likely to cause substantial harm to the individuals affected. If, after a good faith investigation, it's determined that there is not likely a substantial risk of harm, notification is not required.

Third-party agents must notify covered entities within 10 days of discovery of a data breach or a reason to believe that a breach occurred. Covered entities then provide notices to affected consumers and regulatory agencies as required.

### **To Individuals:**

Covered entities must provide written notice to affected individuals within 45 calendar days following the determination that a breach is reasonably likely to cause substantial harm to the individuals affected. Notification is not required if a federal or state agency determines that doing so would undermine a criminal investigation or national security. Notification may be delayed under these circumstances upon written request by the law enforcement agency for a period determined by the agency. Notices must be sent to the mailing address of the individual in the records of the covered entity. Alternatively, an email notice sent to the email address of the individual in the records of the covered entity may be used to notify affected individuals. Notifications must include:

- The actual or estimate date or date range of the breach
- A description of the data affected by the breach

- A description of the actions the covered entity has taken to restore the security and confidentiality of the personal information affected by the breach
- Steps the consumer can take to further protect himself or herself from identity theft
- Contact information consumers can use to obtain more information from the covered entity

Substitute notice may be used when the cost of notification through the standard methods is determined to be excessive (if the cost exceeds \$500,000) or there is lack of sufficient information to notify an individual. If the affected number of consumers exceeds 100,000, covered entities may use both of the following as a substitute notice:

1. A conspicuous notice of the breach, including the required information, on the covered entity's website
2. Notice in print and broadcast media, which includes major broadcast media in both rural and urban areas where the affected individuals reside

With approval of the Attorney General, a substitute form of notification may be used.

### **To Regulators:**

Covered entities and their third-party agents must notify the Alabama Office of the Attorney General if over 1,000 Alabama residents are notified following a security breach. All consumer reporting agencies also must be notified without reasonable delay under the same criteria.

Notice to the Attorney General must include:

- A synopsis of the events surrounding the breach
- The approximate number of affected individuals
- Any services related to the breach that are being offered or scheduled to be offered to the affected individuals without charge, as well as instructions on how to utilize those services
- The name, address, telephone number, and email address of the employee or agent of the covered entity who can provide additional information about the breach

**Covered Information:** Covered information is defined as an individual's first name or first initial and last name in combination with one or more of the following:

- Their Social Security number or tax ID number, driver's license number, state-issued ID card number, or other unique ID number that could be used to verify the individual's identity
- Financial account numbers in combination with security codes, PINs, passwords, expiration dates, or other info necessary to access the account
- Any information disclosing an individual's physical or mental health history, condition, diagnosis, or treatment
- A health insurance policy number or subscriber identification numbers and unique identifiers
- A user name or email address in combination with a password or security question and answer that would provide account access

### **Penalties:**

Violations are considered unlawful trade practices under the Alabama Deceptive Trade Practices Act, Chapter 19, Title 8, Code of Alabama 1975. However, violations do not constitute a criminal offense

under Section 8-19-12, Code of Alabama 1975. Therefore, the Attorney General has the exclusive authority to bring any actions for civil penalties in response to violations.

Any covered entity or third-party agent that knowingly fails to comply with notification requirements are subject to the penalty provisions of Section 8-19-11, Code of 23 Alabama 1975, which may be in amounts up to \$2,000 per violation, not to exceed \$500,000 per breach. A penalty not to exceed \$5,000 per day may be imposed if the entity fails to take reasonable action to comply with the provisions.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Alabama:**

- [Hospital data breach could affect 4.5 million patients](#) – Several Alabama hospitals were impacted by a data breach targeting Community Health Systems, a company that owns 206 hospitals across the U.S., including 11 in the state of Alabama. Data on more than 4.5 million patients who had been treated by the company’s hospitals within the five previous years was stolen. No penalties are reported.

**Pending Data Breach Legislation in Alabama:**

[H.B. 410](#) would create the Data Breach Notification Act, which would “require certain entities to provide notice to certain persons upon a breach of security that results in the unauthorized acquisition of sensitive personally identifying information.”

## Alaska

**Reference:** Alaska Stat. § [45.48.010](#) *et seq.*

**Summary:** In Alaska, a security breach is defined as unauthorized acquisition (or the reasonable belief of such) that compromises the security, integrity, or confidentiality of covered information. This excludes some good-faith acquisitions by employees or agents and applies to businesses with more than 10 employees or any person doing business with another entity who owns, licenses, or maintains covered information. Note that some non-commercial entities may be excluded from these requirements or subject to different requirements.

### **Notification Requirements:**

Notification must be made in the shortest time possible and without unreasonable delay. However, notification may be delayed if a law enforcement agency determines that notice may interfere with a criminal investigation. Additionally, a harm threshold applies: if after investigation it's determined that there is no likelihood of the breach resulting in reasonable harm to the consumer, if written notification of such is provided to the Alaska Attorney General.

### **To Individuals:**

If notification is required, it must be in written form to the individual's most recent postal mailing address. In cases in which the entity communicates primarily with a consumer electronically, electronic notice is acceptable. Electronic notice may also be acceptable if it's consistent with E-SIGN.

Third parties maintaining covered information on behalf of another entity must notify that entity immediately following the discovery of a breach, and they must cooperate in providing any necessary information regarding the breach.

### **To Regulators:**

If more than 1,000 state residents must be notified of a breach, information collectors must also notify all consumer credit reporting agencies. Agencies must be notified without unnecessary delay. Notifications to agencies must include the timing, distribution, and content of the notices provided to residents.

**Covered Information:** First and last name, or a first initial and last name, as well as one or more of the following:

- Social Security number
- Driver's license or state identification card number
- Financial account
- Credit or debit card numbers (along with required security or access codes)
- PINs or passwords that would grant access to financial information
- Passwords, PINs, or other access information for financial accounts

This applies to covered information in both electronic and paper format.

## Penalties:

Alaska has stiff penalties for violations of AS § 45.48.010 – 45.48.090.

Government agencies are liable for civil penalties of \$500 for each resident not notified of a data breach, up to a total possible civil penalty up to \$50,000. However, even if the \$50,000 cap is reached, the agency may still be liable for other violations. For private actions, penalties are limited to the actual economic damages incurred.

Non-government agencies are deemed in violation of unfair or deceptive practice under AS § 45.50.471 – 45.50.561. In this case, the information collector is not subject to civil penalties under AS 45.50.551 but are liable to the state of Alaska for civil penalties up to \$500 per resident not notified, again not to exceed a total civil penalty of \$50,000. Damages awarded against information collectors under AS 45.50.531 are limited to actual economic damages incurred not exceeding \$500, and damages awarded against information collectors under AS 45.50.537 are limited to actual economic damages.

## Special Statutes for Certain Data Types:

None.

## Data Breaches in Alaska:

- [Alaska DHSS settles HIPAA security case for \\$1,700,000](#) – The Alaska Department of Health and Human Services (DHHS) agreed to pay the U.S. Department of Health and Human Services' (HHS) \$1.7 million to settle violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule as well as take corrective actions to improve policies and procedures aimed at securing protected health information (PHI).
- [Data breach at University of Alaska impacts staff, students](#) – A University of Alaska data breach in February 2018 impacted the accounts of 50 people. No penalties are reported.
- [Alaska Office of Children's Services hit with data breach](#) - Alaska Office of Children's Services (OCS) filed a notification that two of its computers had been breached by a [suspected Trojan virus](#) in July 2017, impacting as many as 500 individuals. No penalties are reported.
- [Alaska Communications Acknowledges Data Breach](#) – In January 2014, Alaska Communications notified an undisclosed number of current and former employees of a data breach potentially compromising their names, addresses, birthdates and Social Security numbers as a result of a virus that forwarded data outside the network. No penalties are reported.

## Pending Data Breach Legislation in Alaska:

[S.B. 93](#) is legislation currently pending in Alaska that relates to security freezes on credit reports and other records of certain minors as well as incapacitated individuals.

## Arizona

**Reference:** Ariz. Rev. Stat. § [18-545](#)

**Summary:** Arizona’s data breach notification laws are applicable to individuals or entities that conduct business in the state who also license, own, or maintain covered information. It does not apply to encrypted or redacted information, or information secured in some other way that renders it unreadable or unusable – as long as the encryption key was not accessed or acquired.

A breach is defined as unauthorized access or acquisition that compromises security or confidentiality of covered information. It must either cause or be likely to cause substantial economic loss for the Arizona resident, although it excludes good-faith acquisitions by employees or agents. Various factors must be considered, which are outlined in the Arizona statute.

### **Notification Requirements:**

#### **To Individuals:**

The method of notification may include telephone, written, or electronic notices when this is the primary communication method between the entity and the consumer and the electronic notification is consistent with E-SIGN. Notification must be made as soon as possible and without unnecessary delay. If the entity demonstrates that the cost of providing notice using these methods would exceed \$50,000 or more than 100,000 individuals must be notified, substitute notification may be used including a conspicuous publishing of the notice on the entity’s website or notification to major statewide media.

Any entity that maintains unencrypted data containing personal information that it does not own must notify the owner or licensee of the data without unreasonable delay following discovery of a data breach. The entity maintaining the data must cooperate with the owner or licensee by sharing information relevant to the breach. Note that the person or entity that maintained the breach data is not required to notify individuals affected; the owner or licensee of the data is responsible for notifying affected individuals, unless the agreement between the maintainer and owner or licensee states otherwise.

#### **To Regulators:**

None required.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver’s license or state identification card number
- Financial accounts
- Credit or debit card numbers (plus any security or access codes required)

Covered info in the state of Arizona refers only to electronic information and does not apply to covered information in paper form.



### Penalties:

Entities may be liable for civil penalties for violations. This law may only be enforced by the Arizona Attorney General who may bring an action to obtain actual damages for willful and knowing violations as well as civil penalties up to \$10,000 per breach (or a series of breaches of a similar nature discovered in a single investigation). The same penalties apply to government agencies and non-government agencies in Arizona.

### Special Statutes for Certain Data Types:

[Healthcare data breaches](#) are now covered by Arizona's data breach notification law as of April 2018, with a 45-day notification deadline for notification of individuals.

### Data Breaches in Arizona:

- [Banner Health cyberattack breaches up to 3.7 million records](#) – A 2016 data breach reported by Banner Health impacted up to 3.7 million records. It is facing a [class-action lawsuit](#) as a result of the breach and will face penalties of an unknown amount.

### Pending Data Breach Legislation in Arizona:

[H.B. 2154](#) is legislation currently pending in Arizona relating to personal information and data security breaches. H.B. 2154 would [expand the definition of PI](#), tighten the requirements for notification with a 30-day deadline and also require notification to the Attorney General.

## Arkansas

**Reference:** [Ark. Code §§ 4-110-101 et seq.](#)

**Summary:** In the state of Arkansas, data breach laws apply to any individual or business that acquires, owns, licenses, or maintains covered information. Non-commercial entities may be subject to different requirements, and some entities may be exempt from some or all of the requirements.

The Arkansas Statute does not apply to covered information that is adequately encrypted or redacted, provided that the encryption key has not been accessed or acquired.

A breach is defined as unauthorized access or acquisition that compromises security or confidentiality of covered information. This definition excludes information acquired or accessed in good faith by employees or agents.

### **Notification Requirements:**

#### **To Individuals:**

The method of notification may include written notice or electronic notices when this is the primary communication method between the entity and the consumer and the electronic notification is consistent with E-SIGN. Notification must be made as soon as possible and without unnecessary delay. However, notification may be delayed if a law enforcement agency determines that notice may interfere with a criminal investigation. Additionally, a harm threshold applies: if an investigation determines that there is no reasonable likelihood of harm to consumers, a covered entity is not required to provide notice to affected consumers.

If any individual or business maintains data including personal information that they do not own, they must notify the owner or licensee of the data when any breach occurs immediately following discovery if it's believed that the data was accessed by an unauthorized person.

#### **To Regulators:**

None required.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver's license or state identification card number
- Financial accounts
- Credit or debit card numbers (plus any security or access codes required)
- Medical information

This refers to covered information in electronic form only.

**Penalties:** Civil or criminal penalties may result from violations. Violations under this law are punished through actions by the attorney general, under provisions of deceptive trade practice (§ 4-88-101 et seq.).

### Special Statutes for Certain Data Types:

None

### Data Breaches in Arkansas:

- [Updated: Data breach at Arkansas DHS could affect 26,000 Medicaid beneficiaries; no evidence of ID theft, agency says](#) – Arkansas DHS announced in September 2017 that a spreadsheet containing personal information of 26,044 Medicaid beneficiaries was emailed to an employee’s personal email address. The employee was terminated and the agency was reportedly [pursuing criminal charges](#). No penalties are reported.
- [State department informs Arkansas State of data breach](#) – In May 2014, officials from the Arkansas State University were notified by the Arkansas Department of Human Services of a data breach impacting up to 50,000 individuals. No penalties are reported.
- [Arkansas Oral & Facial Surgery Center notifies 128,000 patients of ransomware incident](#) – In July 2017, the Arkansas Oral & Facial Surgery Center discovered that its computer network had been infected by ransomware. More than 128,000 patients were notified of the breach, although the patient information database was not impacted except for a limited number of patients. No penalties are reported.

### Pending Data Breach Legislation in Arkansas:

None

## California

**Reference:** Cal. Civ. Code §§ [1798.29](#), [1798.82](#)

**Summary:** Any person or business that does business in the state of California and owns, maintains, or licenses covered information is subject to California’s data breach laws. Certain types of businesses may be exempt from some or all of the requirements. Non-commercial entities may be subject to different requirements.

A data breach is defined as the unauthorized acquisition of covered information that compromises the security, integrity, or confidentiality of covered information. This excludes some good-faith acquisitions by employees or agents.

### Notification Requirements:

#### To Individuals:

Notification must be made as soon as possible without unnecessary delays. Notices must contain plain language and use a 10-point font size or larger, as well as the following information:

- Name and contact information for the covered entity
- Types of covered information that were breached
- Date or estimated date range of the breach
- Date of the notice
- Whether notification was delayed due to law enforcement deeming that notification would interfere with an investigation
- A general description of the breach
- Toll-free numbers and addresses for entities or agencies that manage Social Security numbers, driver’s licenses, and related information if such information was breached

The statute does not apply to information that is encrypted, provided that the encryption key is not acquired or accessed. Notification must be provided either in written form or electronic format consistent with E-SIGN.

Note that in California, covered entities must also provide identify theft prevention and mitigation services at no charge for a minimum of 12 months if a breach includes Social Security numbers, driver’s license numbers, or state identification card numbers.

#### To Regulators:

Individuals and businesses that are required to issue a security breach notification to more than 500 California residents must submit a single sample copy of the notification provided to consumers (with personal information redacted) to the attorney general.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver’s license or state identification card number

- Financial accounts
- Credit or debit card numbers (plus any security or access codes required)
- Medical or health insurance information
- Information collected by automated license plate recognition systems

Additionally, covered information includes a username or email address in combination with passwords or security question responses that would grant access to a resident's online account.

Covered information includes information in electronic format only.

### **Penalties:**

Civil penalties may apply for violations. Consumers who are injured by a violation of this law have the right to initiate a civil action to recover any damages they suffered as a result. This right does not apply to individuals impacted under the medical information-specific statute in California. Under the medical information-specific statute, the California Department of Health and Human Services may impose penalties on covered entities including:

- A \$25,000 penalty per patient whose information was compromised
- A penalty of up to \$17,500 per subsequent occurrence of unauthorized or unlawful access, use, or disclosure of personal medical information
- If required notification is not provided, a penalty of \$100 per day after the initial 15-day period may apply

Total penalties for a single event are not to exceed \$250,000.

### **Special Statutes for Certain Data Types:**

California has a statute specific to medical information: [Cal. Health & Safety Code § 1280.15](#)

This statute applies to clinics, health facilities, home care agencies, and hospice providers which are licensed under sections 1204, 1250, 1725, or 1745 of the Cal. Health & Safety Code. It's applicable to patient medical information including any information in printed or electronic form that is personally identifiable and relates to the patient's medical history, physical or mental health conditions, or treatment. This information may include:

- Name
- Address
- E-mail address
- Telephone number
- Social Security number
- Any other information that reveals the individual's identity alone or in combination with other information that's already publicly available

In the case of medical information, the notification requirement is triggered by any unlawful or unauthorized access, use, or disclosure of a patient's medical information. Unlike non-medical data, the medical information statute does not stipulate specific exemptions for data that is encrypted, redacted, or made unreadable through some other method. Covered entities are required to notify individuals within 15 days of discovery of the breach, and they also must notify the California Department of Health

Services within the same 15 days. Different penalties exist for breaches of medical information as described above.

#### **Data Breaches in California:**

The California Office of the Attorney General maintains a [searchable database](#) of reported breaches in the state.

- [California Data Breach Prompts Warning For State Employees](#) – A former state employee downloaded sensitive information of thousands of state employees, exposing the affected individuals to potential identity theft. The breach occurred in late 2017 and is under investigation. No penalties are reported.
- [Uber Broke California Law by Concealing Massive Data Breach, L.A. City Attorney Alleges in Lawsuit](#) – In October 2016, hackers stole the names, cell phone numbers, and email addresses of more than 57 million Uber users around the world in addition to driver's license numbers of more than 600,000 drivers. Uber failed to notify the drivers affected in the state of California. A lawsuit is pending, but no penalties are yet reported.
- [Breach at Sabre Corp.'s Hospitality Unit](#) – Sabre Corp. disclosed a potentially significant data breach of payment and customer data tied to travel bookings that were processed by a reservation system that serves more than 32,000 lodging establishments in May 2017. No penalties are reported.

#### **Pending Data Breach Legislation in California:**

California Governor Jerry Brown signed [AB-375](#) in June 2018. It is slated to go into effect January 1, 2020. The law will mandate a company, upon request, to tell customers what information it has on them. Consumers will also be able to ask companies to delete any data they may have on them and opt out of having that data sold.

The bill would apply to companies with data on more than 50,000 people and intentional violations would carry a \$7,500 fine. In both consumer and state lawsuits, companies would be given 30 days to fix the problem.

For breaches, consumers would be able to sue up to \$750 for each violation according to section 1798.150 of the bill.

## Colorado

**Reference:** [Colo. Rev. Stat. § 6-1-716](#)

**Summary:** Any person or business that does business in the state of Colorado and owns, maintains, or licenses covered information is subject to Colorado’s data breach laws. Certain types of businesses may be exempt from some or all of the requirements. Non-commercial entities may be subject to different requirements.

A data breach is defined as the unauthorized acquisition of covered information that compromises the security, integrity, or confidentiality of covered information. This excludes some good-faith acquisitions by employees or agents.

The statute does not apply to encrypted or redacted information, or information secured in some other way that renders it unreadable or unusable – as long as the encryption key was not accessed or acquired.

### **Notification Requirements:**

#### **To Individuals:**

The method of notification may include written notice, telephone notice, or electronic notices when this is the primary communication method between the entity and the consumer and the electronic notification is consistent with E-SIGN. Notification must be made as soon as possible and without unnecessary delay. However, notification may be delayed if a law enforcement agency determines that notice may interfere with a criminal investigation and law enforcement notifies the covered entity of such.

Additionally, a harm threshold applies: if an investigation determines that there has been no misuse of a consumer’s covered information and misuse is not reasonably likely to occur, notification is not required.

#### **To Regulators:**

If a covered entity is required to notify more than 1,000 Colorado residents of a data breach, the entity must also notify all nationwide consumer credit reporting agencies of the anticipated date of notification to the affected individuals as well as the approximate number of Colorado residents that will be notified.

Individuals and entities that maintain covered information on behalf of another organization must provide immediate notice to the entity maintaining primary responsibility for the information – if misuse of the covered info has already occurred or is reasonably likely to occur. If more than 1,000 residents are notified, all nationwide consumer reporting agencies (CRAs) also must be notified without delay.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver’s license or state identification card number

- Financial accounts
- Credit or debit card numbers (plus any security or access codes required)

This includes covered information in electronic form only.

**Penalties:**

Violations may result in civil penalties, as determined by the Attorney General who has the authority to bring actions in law or equity in response to violations, or for any other appropriate relief that can aid in ensuring compliance or recovering economic damages suffered as a direct result of the violation.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Colorado:**

- [State juror pool data breach exposed Social Security numbers](#) – In July 2017, an Alaska resident alerted state officials to the possibility of a data breach resulting in the risk of identity theft. The breach exposed 620,945 names, as well as corresponding Social Security numbers and dates of birth, on the Judicial Department’s internal intranet. Names and other data comprising 41,140 records were exposed externally on the worldwide web. The information had been exposed for nearly a year, since August 2016. No penalties are reported.

**Pending Data Breach Legislation in Colorado:**

[H.B. 1128](#), which concerns strengthening the protections for the privacy and security of consumer data. The Governor of Colorado signed this into effect in May 2018. It goes into effect September 1, 2018.



## Connecticut

**Reference:** Conn. Gen Stat. §§ [36a-701b](#), [4e-70](#)

**Summary:** In the state of Connecticut, data breach laws apply to any individual or business that acquires, owns, licenses, or maintains covered information. Non-commercial entities may be subject to different requirements, and some entities may be exempt from some or all of the requirements.

The statute does not apply to encrypted or redacted information, or information secured in some other way that renders it unreadable or unusable – as long as the encryption key was not accessed or acquired.

In Connecticut, a data breach is defined as unauthorized access or acquisition of covered information.

### Notification Requirements:

#### To Individuals:

The method of notification may include written notice, telephone notice, or electronic notices consistent with E-SIGN. Notification must be made as soon as possible and without unnecessary delay. However, notification may be delayed if a law enforcement agency determines that notice may interfere with a criminal investigation and requests that notification to consumers be delayed. Additionally, a harm threshold applies: if an investigation determines that no harm to affected residents is likely to occur as a result of the breach, notification is not required.

Note that in Connecticut, covered entities must also offer to provide appropriate identity theft prevention and mitigation services at no charge for 12 months or more if Social Security numbers were breached. Information on how to place a credit freeze on the individual's credit file must also be provided.

#### To Regulators:

A covered entity in Connecticut must also notify the Connecticut Attorney General of a data breach no later than when affected consumers are notified. Entities maintaining covered info on behalf of another covered entity must notify the covered entity immediately of a breach.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver's license or state identification card number
- Financial accounts
- Credit or debit card numbers (plus any security or access codes required)

This includes covered information in electronic form only.

**Penalties:** Civil penalties may apply to violations, which are considered an unfair trade practice under 42-110b. Violations are enforced by the Attorney General. The statute defers to the federal courts and the Federal Trade Commission.

### Special Statutes for Certain Data Types:

None

### Data Breaches in Connecticut:

- [Colorado's OIT notifies 3,000 residents of data breach](#) – In August 2015, Colorado's Office of Information Technology notified 3,000 residents of a data breach resulting from a technical error, in which letters containing residents' personal information were mailed to the wrong address. The letters included 1,622 letters intended for Medicaid recipients and included names, addresses, state identification numbers, income information, and other personally identifiable information. An additional 1,069 letters intended for Colorado Department of Human Services (CDHS) clients contained names, addresses, and state identification numbers. No penalties are reported.

### Pending Data Breach Legislation in Connecticut:

[S.B. 472](#) relates to fees for security freezes on credit reports, notification of consumers' decision to remove or place a security freeze on a credit report, as well as the duration of identity theft protection services required following a data breach. This legislation would prohibit credit reporting agencies from charging a fee for placing or removing security freezes and require credit rating agencies to notify other credit rating agencies of freeze requests received from consumers.

## Delaware

**Reference:** Del. Code [tit. 6, § 12B-101 et seq.](#)

**Summary:** In the state of Delaware, data breach laws apply to any individual or business that owns, licenses, or maintains covered information. Non-commercial entities may be subject to different requirements, and some entities may be exempt from some or all of the requirements.

The statute does not apply to encrypted information, as long as the encryption key was not accessed or acquired.

A data breach is defined as the unauthorized acquisition of covered information that compromises the security, integrity, or confidentiality of covered information. This excludes some good-faith acquisitions by employees or agents.

### Notification Requirements:

#### To Individuals:

The method of notification may include written notice, telephone notice, or electronic notices consistent with E-SIGN. Notification must be made as soon as possible and without unnecessary delay. However, notification may be delayed if a law enforcement agency determines that notice may interfere with a criminal investigation. Additionally, a harm threshold applies: if an investigation determines that no harm to affected residents is likely to occur (and has not already occurred) as a result of the breach, notification is not required.

#### To Regulators:

If more than 500 Delaware residents are affected and must be notified, the covered entity must also provide notice to the Delaware Attorney General no later than when notice is provided to individuals.

Third-party entities that maintain covered information on behalf of a covered entity must notify the covered entity of a breach immediately as well as provide any necessary information about the breach.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver's license or state identification card number
- Financial accounts
- Credit or debit card numbers (plus any security or access codes required)

This includes covered information in electronic form only.

**Penalties:** Entities may be liable for civil penalties for violations. "Appropriate damages and penalties" for violations are at the discretion of the Attorney General. Private actions are permitted by individuals with a cap of triple the damages plus costs and attorney's fees. If breached data includes social security numbers, the entity is required to provide credit monitoring services for at least one year to any affected individual whose social security number was compromised or believed to have been

compromised, unless if, following an appropriate investigation, it's determined that the breach is unlikely to result in harm to the affected individuals.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Delaware:** The Delaware Attorney General's Office maintains a [database of data breaches](#) impacting Delaware residents.

- [Delta and Sears say data breach exposed hundreds of thousands of credit cards](#) – An online support services company, [24]7, suffered a malware attack from September 26 or 27 to October 12, 2017, potentially impacting customers who made online purchases from Delta or Sears during that period. The data at risk included credit card information. Sears reported that the breach impacted less than 100,000 customers, while in all, it's believed that hundreds of thousands of customer records were potentially compromised. No penalties are reported.
- [Notice of Unauthorized Access or Acquisition to Chili's Grill & Bar Guest Area](#) – Guest payment information was compromised at certain Chili's restaurant locations. The data incident is believed to be limited to a period between March and April 2018, although the company is still investigating to determine the scope of the incident. No penalties are reported.

**Pending Data Breach Legislation in Delaware:**

None

## Florida

**Reference:** Fla. Stat. §§ [501.171](#), [282.0041](#), [282.318\(2\)\(i\)](#)

**Summary:** In the state of Florida, data breach laws apply to any individual or business that acquires, maintains, stores, or uses covered information. Non-commercial entities may be subject to different requirements, and some entities may be exempt from some or all of the requirements.

The statute does not apply to encrypted or redacted information, or information secured in some other way that renders it unreadable or unusable – as long as the encryption key was not accessed or acquired.

A data breach is defined as unauthorized access of covered information, with the exception of certain situations in which information is accessed in good faith by employees or agents.

### **Notification Requirements:**

#### **To Individuals:**

Notifications must be in the form of written communication or email and must include:

- Date(s) of the breach
- A description of the covered info accessed or believed to be accessed
- Contact information for the covered entity

If law enforcement determines that a breach would impede a criminal investigation and provides a written request, notification may be delayed. Additionally, if investigations by federal, state, or local law enforcement determine that no harm has resulted to residents impacted by the breach and no harm is likely to result, notification is not necessary. This decision must be documented in writing and maintained for a period of at least five years.

#### **To Regulators:**

Covered entities must also immediately notify the Florida Department of Legal Affairs if 500 or more individuals are affected by a breach, no later than 30 days following the identification of a breach. An additional 15 days may be provided for good cause when a reasonable cause is communicated in writing. If more than 1,000 residents are impacted by a breach, all nationwide CRAs must be notified without unreasonable delay.

Third parties that maintain covered information on behalf of a covered entity must notify the entity no later than 10 days from determination of the breach, but as promptly as possible. This notice must provide all information the entity requires to comply with the requirements of the notice.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver's license or state identification card number
- Military identification

- Any other form of identification that can be used to verify the individual's identity
- Financial accounts
- Credit or debit card numbers (plus any security or access codes required)
- Medical information, including mental/physical conditions, medical treatment or diagnosis
- Health insurance policies or subscriber identification numbers and any unique identifier used by medical providers
- Information collected by automated license plate recognition systems

Additionally, covered information includes a username or email address in combination with passwords or security question responses that would grant access to a resident's online account.

Covered information includes information in electronic format only.

**Penalties:** Civil penalties may result from violations. Violations are considered unfair or deceptive trade practices, and penalties provided for under s. 501.207 apply. Additionally, covered entities that violate notification requirements are liable for civil penalties not to exceed \$500,000 – up to \$1,000 per day for each day, up to the first 30 days, following a violation and \$50,000 for each subsequent 30-day period or a portion thereof for up to 180 days.

If the violation exceeds 180 days, penalties in an amount not to exceed \$500,000 may apply. Civil penalties are per breach, not per affected individual, and penalties collected under these provisions are deposited into the General Revenue Fund. No private cause of action is provided.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Florida:**

- [Data breach in Florida leads to tighter cybersecurity controls at the FDIC](#) – A total of eight major security breaches impacted various branches of the FDIC in 2015 and 2016, including one major breach in the Gainesville office in 2015. A total of 121,633 bank customers at 380 financial institutions were impacted. While no penalties are reported, a [House committee is now investigating](#) the series of breaches at the FDIC following a breach resulting from a former employee with a mobile storage device that contained personal data on more than 44,000 individuals.

#### **Pending Data Breach Legislation in Florida:**

None

## Georgia

**Reference:** [Ga. Code](#) §§ 10-1-910, -911, -912; § 46-5-214

**Summary:** In Georgia, laws pertaining to data breaches are applicable to data collectors – such as certain government entities – as well as information brokers, defined as any business or individual who collects, assembles, evaluates, compiles, reports, transmits, transfers, or communicates any information to provide this information to unaffiliated third parties.

A data breach is defined as the unauthorized acquisition of covered information that compromises the security, integrity, or confidentiality of covered information. This excludes some good-faith acquisitions by employees or agents.

The law does not apply to information that is encrypted or redacted, provided that the encryption key has not been accessed.

### **Notification Requirements:**

#### **To Individuals:**

When a breach occurs, notification must be prompt and without any unreasonable delay. Notification may take place via written, telephone, or electronic notification, if consistent with E-SIGN.

Notification may be delayed if law enforcement determines that notification would compromise a criminal investigation. However, after law enforcement determines that notification will no longer compromise an investigation, notification must be carried out.

#### **To Regulators:**

If more than 10,000 consumers are impacted by a breach, all nationwide CRAs must be notified without delay. This notification must include information on the timing, content, and distribution of the notice provided to consumers.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver's license or state identification card number
- Credit or debit card numbers (if it can be used without any additional information, passwords, or access codes)
- Account passwords, PINs, and access codes

Even if not accompanied by a first and last name or first initial and last name, any of the above items would constitute covered information if the information can be used to attempt or perform identity theft as-is.

The information outlined above is only considered covered information in electronic form.

**Penalties:** Civil penalties may result from violations. Violations may be prosecuted under the Fair Business Practices Act, with fines not to exceed \$100 for a violation related to a specific consumer.

### Special Statutes for Certain Data Types:

None

### Data Breaches in Georgia:

- [Orthopedic practice breach hits half-million patients](#) – In 2016, Peachtree Orthopedics was hit with one of the largest data breaches to occur in Georgia, with the records of more than 500,000 patients compromised in the attack. It was the largest breach of a medical-related group in the state to date in 2016, and the sixth largest in the U.S. health care sector in 2016. Names, addresses, email addresses, and in some cases, Social Security numbers were stolen in the breach. No penalties are reported.

### Pending Data Breach Legislation in Georgia:

[H.B. 499](#) would enact the Personal Data Security Act and improve systems and procedures for providing and regulating data breach notifications. It would also revise legislative findings and declarations, as well as definitions and when notices of breaches are required. Additionally, it would provide for the content of notices and require certain entities to maintain certain data security procedures, as well as require notices to be sent to certain officials.

[H.B. 82](#) relates to the notification required following a security breach involving personal information, requiring data brokers and collectors to provide notice when data is released to unauthorized persons, whether it is intentional, inadvertent, or accidental. It would also repeal conflicting laws.



## Hawaii

**Reference:** Haw. Rev. Stat. § [487N-1 et seq.](#)

**Summary:** Commercial entities that own, license, or maintain covered information are subject to Hawaii's data breach laws. Certain businesses may be exempt from some or all requirements, and different requirements may apply to non-commercial entities.

The law does not apply to information that has been encrypted, provided that the encryption key has not been acquired or accessed.

A breach is defined as unauthorized access or acquisition of information when illegal use of the information either has occurred or is likely to occur. It must create a risk of harm to the individual. Good-faith access by employees or agents may be exempt in some cases. In Hawaii, a harm threshold applies: an incident constitutes a breach only when illegal use of covered information has occurred or is likely to occur and creates a risk of harm to the individual.

### **Notification Requirements:**

#### **To Individuals:**

Consumers must be notified of a breach as soon as possible and without unnecessary delay. Hawaii also specifies the content that a notice must contain, including clear and concise information regarding the type of covered information that was accessed or acquired, a general description of the incident, what actions a consumer should take to prevent their covered information from further access or misuse, and a telephone number that consumers can call for further information and assistance.

Written notices must be mailed to the consumer's last known address, although notification may also be conducted by telephone (if direct contact is made) or electronically via email if consistent with E-SIGN and the consumer has consented to receiving email communications from the entity.

Note that notification may be reasonably delayed should law enforcement determine that notifying consumers could impede a criminal investigation or jeopardize national security and provides written notice of these concerns. The delay request must be in writing or documented clearly by the covered entity.

#### **To Regulators:**

If more than 1,000 consumers are notified of a breach, the covered entity must also notify the Hawaii Office of Consumer Protection in writing, as soon as possible. Third parties that maintain covered information on behalf of another entity must notify that entity promptly following a breach.

Additionally, if the same criteria are met (1,000 individuals receiving notification), all nationwide CRAs must be notified in writing as well.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver's license or state identification card number

- Credit or debit card numbers, account passwords, or access codes that would permit access to an individual's financial account

The information above is considered covered information in both electronic and paper form.

**Penalties:** Civil penalties may apply for violations. Violations of any provision of this chapter are subject to penalties of up to \$2,500 per violation. Actions may be brought by the Attorney General or the executive director of the Office of Consumer Protection. In addition, covered entities are also liable to the injured parties in an amount equaling the sum of actual damages directly resulting from the violation. The courts may award reasonable attorneys' fees to the prevailing party.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Hawaii:**

- [Massive data breach impacts all Zippy's Restaurants](#) – Between November 23, 2017 and March 29, 2018, all Zippy's restaurant locations were impacted by a data breach of its credit and debit card processing system. Compromised information may include names, card numbers, expiration dates, and security codes of credit and debit cards used at any Zippy's location during that time frame. The state's Office of Consumer Protection is investigating the incident, although no penalties are reported at this time.

**Pending Data Breach Legislation in Hawaii:**

[S.B. 2259](#) would require state consumers who receive a summary of rights under the Fair Credit Reporting Act to receive a notice of their rights under Hawaii law to obtain a security freeze on their credit reports.

[H.B. 2342](#) and [S.B. 2769](#) would eliminate the fee charged by a consumer reporting agency to place, lift, or remove a security freeze requested by a consumer and allow consumers to request a security freeze at any time.

## Idaho

**Reference:** Idaho Stat. §§ [28-51-104 to -107](#)

**Summary:** Commercial entities that own, license, or maintain covered information are subject to Idaho's data breach laws. Certain businesses may be exempt from some or all requirements, and different requirements may apply to non-commercial entities.

The statute does not apply to covered information that has been encrypted, unless encryption keys have been accessed or acquired.

A data breach is defined by the state of Idaho as an illegal acquisition of information that compromises the security, integrity, or confidentiality of covered information. This excludes some good-faith acquisitions by employees or agents.

### **Notification Requirements:**

#### **To Individuals:**

Notification must be carried out as promptly as possible. Written notices must be mailed to the consumer's last known address, although notification may also be conducted by telephone (if direct contact is made) or electronically via email if consistent with E-SIGN and the consumer has consented to receiving email communications from the entity. Note that notification may be reasonably delayed should law enforcement determine that notifying consumers could impede a criminal investigation.

Notification is not required if an investigation determines that there is not a reasonable risk to the consumer that their information has been or will be misused. If a third-party maintains covered information on behalf of another entity, this entity must be notified immediately following a breach.

#### **To Regulators:**

State agencies are required to inform the Idaho Attorney General within 24 hours of the discovery of a data breach.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver's license or state identification card number
- Credit or debit card numbers, as well as any additional information that would permit access to an individual's financial account

This applies only to covered information in electronic form.

**Penalties:** Violations may result in civil penalties. When a primary regulator for an agency, commercial entity, or individual has reason to believe that that entity, agency, or individual has violated section 28-51-105, Idaho Code by failing to provide required notification, that regulator may bring a civil action. Violators are subject to fines not to exceed \$25,000 per breach.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Idaho:**

- [Idaho school works to recover data weeks after cyberattack](#) - Jerome School District in Idaho experienced a ransomware attack in December 2017, and as of January 2018, the district was still working to recover its data. The requested ransom was the equivalent of \$65,000, although the district opted not to pay it, believing that the data could be recovered through backups. No penalties are reported.
- [Attorney General Urges Consumers to Take Precautions after T-Mobile Data Breach](#) – In 2015, thousands of Idaho consumers were impacted by a data breach of a third-party server hosting data for T-Mobile. In total, 55,000 consumers were at risk of having their personal data exposed, and stolen data included names, addresses, Social Security numbers, birth dates, passport numbers, and information used in T-Mobile credit assessments. No penalties are reported.

**Pending Data Breach Legislation in Idaho:**

None

## Illinois

**Reference:** 815 ILCS §§ [530/1 to 530/25](#)

**Summary:** Commercial entities that own, license, or maintain covered information are subject to data breach laws in the state of Illinois. Certain businesses may be exempt from some or all requirements, and different requirements may apply to non-commercial entities.

If the acquired information is encrypted or redacted, it does not constitute a breach unless the encryption key has also been accessed or acquired.

A data breach is defined by the state of Illinois as unauthorized access or acquisition of information that compromises the security, integrity, or confidentiality of covered information. This excludes some good-faith acquisitions by employees or agents.

### **Notification Requirements:**

#### **To Individuals:**

Notification must be carried out as promptly as possible either in writing or electronically if consistent with E-SIGN and the consumer has consented to receiving email communications from the entity. However, if the breach involves user names or email addresses, electronic notification is considered acceptable even if not compliant with E-SIGN in order to direct affected individuals to change their usernames, passwords, and security questions as applicable.

There are also some content requirements in Illinois regarding what information must be included in a consumer notice:

- Toll-free numbers and addresses for CRAs
- Toll-free number, address, and website for the FTC
- A statement that discloses to the consumer that information on fraud alerts and security freezes may be obtained by contacting CRAs and the FTC

Additionally, the notification may NOT include any details about the number of Illinois residents impacted by the breach.

Note that notification may be reasonably delayed should law enforcement determine that notifying consumers could impede a criminal investigation. Law enforcement must request this delay in writing.

#### **To Regulators:**

The Attorney General must be notified by covered entities and business associates within 5 days of notifying the U.S. Department of Health and Human Services (HHS), if HHS notification is required for a breach under the HITECH Act.

If a third party maintains covered information on behalf of another entity, this entity must be notified immediately following a breach, and the third party must cooperate and communicate in regard to the breach.

**Covered Information:** Covered information includes first and last name or first initial and last name plus one or more of the following:

- Social Security number
- Driver's license or state identification card number
- Credit or debit card numbers, as well as any additional information that would permit access to an individual's financial account
- Medical or health insurance information
- Unique biometric data that can be used to authenticate an individual including fingerprints, retina or iris images, or any other unique digital or physical representation

This applies only to covered information in electronic form.

**Penalties:** Civil penalties may apply if violations occur. Violations are considered unlawful practices under the Consumer Fraud and Deceptive Business Practices Act and are subject to all applicable penalties under the CFDBPA. Enforcement powers fall under the Attorney General of Illinois, who may seek remedies including injunction, revocation of the right to do business in the state of Illinois, restitution, and civil penalties up to \$50,000.

If a court deems the entity's actions were meant to defraud, the court may impose a civil penalty up to \$50,000 per violation. Additional penalties of up to \$10,000 per violation may be imposed for violations against individuals 65 years of age or older (815 ILCS 530/20; 505/7). Additionally, any individual who has suffered actual damages may bring a civil action under the Consumer Fraud and Deceptive Business Practices Act (815 ILCS 505/10a).

#### **Special Statutes for Certain Data Types:**

None. See [Pending Data Breach Legislation in Illinois](#) for information on pending legislation pertaining to student and minor data.

#### **Data Breaches in Illinois:**

- [5.4 million Illinois residents affected by massive Equifax data breach](#) – The Equifax data breach affected more than 5.4 million Illinois residents in the September 2017 breach. Compromised data included Social Security numbers, birth dates, addresses, driver's license numbers, and phone numbers, as well as some individual credit card account numbers. Several lawsuits have been filed against Equifax as a result of this massive breach.
- [Illinois Hospital Breach Exposes up to 9,000 Patients' Data](#) – Silver Cross Hospital in New Lenox, Illinois experienced a data breach that compromised the personal data of approximately 9,000 patients. The incident actually resulted from an incident impacting a third-party vendor that managed parts of the hospital's website. The breach was discovered in June 2017, and as of August, 2017, officials were reporting that there was no evidence that unauthorized individuals had gained access to the compromised data. No penalties are reported.

#### **Pending Data Breach Legislation in Illinois:**

[H.B. 332](#) relates to student data privacy, amending the School Student Records Act and sets forth provisions that allow for the disclosure of student records to researchers at an accredited post-

secondary institution or another organization conducting research provided that specified requirements are met. It would also amend the Children's Privacy Protection and Parental Empowerment Act to modify the definition of child as a person under age 18.

[H.B. 3872](#) would amend the Consumer Fraud and Deceptive Business Practices Act. It provides that in addition to freezing a minor's credit report, a freeze may also be placed on the minor's credit file. It also establishes procedures for obtaining a freeze on a credit file for a minor or protected consumer and defines terms.

[H.B. 4095](#) amends the Consumer Fraud and Deceptive Business Practices Act, prohibiting the imposition of a charge on a consumer for placing, removing, or temporarily lifting a credit report freeze.

[S.B. 2018](#) would create the Student Data Privacy Act, requiring a school district's board to enter into a written contract with a contractor when the board shares or provides the contractor with access to student information, records, or student-generated content. Additionally, it would set forth provisions related to contract requirements and security breach procedures, as well as the establishment of a task force.

[S.B. 2230](#) would amend the Consumer Fraud and Deceptive Business Practices Act. It prohibits consumer reporting agencies from charging consumers for placing, removing, or temporarily lifting a freeze.

[S.B. 3007](#) would amend the Personal Information Protection Act. It provides that a data collector required to report breaches to more than 100 residents resulting from a single breach must also report the breach to the Attorney General, and also provides that the Attorney General would issue annual reports to the General Assembly with specified information regarding data security breaches.

[S.B. 3201](#) would amend the School Student Records Act. Upon the discovery of a security breach resulting in unauthorized disclosure or acquisition of student information contained in a school record, S.B. 3201 would require a school to notify the parent of the affected student(s) no later than 48 hours following discovery of the breach.

[H.B. 4174](#) would amend the Personal Information Protection Act. It would require data collectors that own or license personal information of residents and any state agency collecting personal information concerning residents to notify the resident of security breaches within 48 hours of discovery.

[H.B. 4367](#) would amend the Personal Information Protection Act. It provides that any private entity data collector that owns or licenses personal information pertaining to residents must notify affected residents no later than 14 days following discovery of the data breach.

## Indiana

**Reference:** Ind. Code §§ [4-1-11 et seq.](#), [24-4.9 et seq.](#)

**Summary:** In Indiana a security breach is defined as an unauthorized acquisition of computerized data which compromises the confidentiality, security or integrity of a resident's personal information. Any breach that involves paper documents that were at any time maintained as computerized data are also covered.

### **Notification Requirements:**

An unauthorized acquisition of computerized data that compromises the integrity, confidentiality or security of personal information that is maintained by a state or local agency is termed as a breach in the security of the system and must be made aware without unreasonable delay.

The notification is not applicable for acquisition of information in good faith by an agency and for data which is not used further towards any unauthorized disclosure.

### **To Individuals:**

The disclosure of a security breach needs to be congruent with the actual needs of law enforcement and the entity needs to take reasonable steps to measure the scope of the security breach to restore and maintain integrity of the data system.

The database owner needs to disclose the breach of security to an Indiana resident whose unencrypted personal information could have been accessed by an unauthorized person or the encrypted personal information has been acquired by some unauthorized personnel with access to the encryption key.

A state agency may provide notice in writing or by electronic mail (if the individual has provided the email address). A state agency may use an alternate form of notification if the cost of sending notifications to Indiana residents is at least \$250,000, the number of persons to notify exceeds 500,000 or the agency does not have sufficient contact information for each resident.

### **To Regulators:**

The notification to regulators could be delayed if a law enforcement agency deduces that the notification will hamper a criminal investigation. However, if the law enforcement agency concludes that the notification will no longer compromise the investigation, it needs to be sent immediately.

The database owner if required to make a disclosure to more than 1000 affected residents shall also disclose to every reporting agency of the consumer the information required to prevent fraud and also disclose to the attorney general the information of an Indiana resident who is affected by the breach of the security of the system.

**Covered Information:** Personal information consists of first name and last name or first initial and last name combined with one or more data elements that discloses a person's identity such as:

- Social security number
- Driver's license number or identification card number
- Account number, credit card number or debit card number
- Password, security code or access code of an individual's financial account



The covered information does not include:

- The last 4 digits of an individual's social security number
- Any information that is legally available in the public records of a federal or local agency

**Penalties:**

A person or organization that fails to comply with the provision of the disclosure or commits a deceptive act (failure to make a required disclosure) is susceptible to action only by the attorney general. The attorney general may apply a civil penalty of not more than \$150,000 per deceptive act or an injunction to enjoin future violations subject to investigation of the deceptive act.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Indiana:**

- [Indiana Family and Social Services Administration](#) – In 2013, 188,000 clients of Indiana family and social service administration were notified of a breach of their personal information due to a computer programming error by a business associate.
- [Jason's Deli](#) – In Dec 2017, Jason's deli announced a possible breach resulting in customer information such as confidential credit card data appearing on the dark web.
- [Indiana Medicaid](#)—A report containing personal medical information was accessible via a live hyperlink to the public which exposed medical records since 2017.

**Pending Data Breach Legislation in Indiana:**

None

## Iowa

**Reference:** Iowa Code §§ [715C.1](#), [715C.2](#)

**Summary:** For the state of Iowa, a breach of security refers to an access of personal information that is maintained with confidentiality and security by a person or an organization. It also refers to unauthorized access of personal information maintained in paper or any other electronic medium.

Access to the confidential information in good faith by an employee or agent for a legitimate purpose does not count as a breach if the data is not used in violation of a law or the information used does not pose a threat to the person's integrity and security.

### **Notification Requirements:**

A person or organization owning personal information for various needs such as vocation, business, volunteering or occupation purpose needs to give notice of the breach of security without unreasonable delay and consistent with the legal requirements of law enforcement.

### **To Individuals:**

Any person maintaining information on behalf of another person shall notify the licensor or owner immediately if a customer's information was a part of the information that was breached. The notification to the end consumer could be delayed if a law enforcement agency states that the delay will not compromise or hinder the criminal investigation.

A written notice needs to be sent to the last available address of the Iowa resident's records. An electronic notice can also be sent if that is the resident's preferred method of communication. A substitute notice could be sent if the cost of providing notice exceeds \$250,000, if the consumers affected are greater than 350,000 people or there is not sufficient contact information to provide notice. Substitute notice needs to constitute of an email notice, posting on the internet site of the person if the affected person has an internet site and a notice to media outlets across Iowa.

### **To Regulators:**

A person who possesses computerized personal information and is subject to breach of security that requires notification to more than five hundred residents of the state of Iowa, shall also give written notice to the director of the consumer protection division of the attorney general within five business days following the breach of security.

**Covered Information:** Personal information that includes a person's first name or first initial and last name in combination with one of the following data elements:

- Social security number
- Driver's license number or unique identification number
- Any financial account number along with a combination of its access code or password
- Routing code or electronic identifier with a combination of its security or access code
- Unique biometric data such as a retina image or fingerprint

### **Penalties:**

A violation or an unlawful practice could result in the attorney general seeking damages from the person held responsible for the security breach on behalf of the consumer injured by the violation.

### Special Statutes for Certain Data Types:

None

### Data Breaches in Iowa:

- [DHS Data Breach](#): Iowa department of human services reported to the state agency of a phishing email campaign that resulted in hackers having access to email accounts.
- [Health care data breach](#): An email breach was announced which allowed hackers access to personal data from credit card information to social security numbers.
- [Nationwide Mutual Insurance](#): Nationwide insurance company paid \$5.5 million as a part of a settlement that affected more than a million customers. The personal data included social security, driver's license and credit scores that were compromised.

### Pending Data Breach Legislation in Iowa:

[S.B. 2177](#) relates to consumer data protection and the freeze of personal information for security breach protection.

## Kansas

**Reference:** Kan. Stat. § [50-7a01 et seq.](#)

**Summary:** In Kansas, a security breach refers to an unauthorized access of unencrypted data or personal information that is maintained by an individual or organization that results in an identity theft of a customer. Obtaining data in good faith by an agent or employee that is not subject to further unauthorized disclosure does not constitute as a breach of the security of the system.

### Notification Requirements:

A person or entity needs to conduct a prompt investigation to determine the misuse of the information as soon as it is made aware of a security breach.

### To Individuals:

If the investigation deduces that the personal information can be misused the person or entity needs to give a notice immediately to the Kansas resident without unreasonable delay. The notice can be delayed if an agency concludes that it is likely to hinder a criminal investigation. The notification must be made in good faith and without delay as soon as the law information agency determines that it will no longer impede the investigation.

The notification requirements are bearing on any commercial entity that is regulated by federal or state law and maintains procedures for regulations, rules, guidance and laws for a breach in security.

### To Regulators:

If a person discovers that the notification needs to be sent to more than a 1000 consumer simultaneously the person must also notify all consumer reporting agencies that maintain files and compile information on a nationwide basis without unreasonable delay. The attorney general has the power to bring to action the necessary law and relief to action as may be appropriate.

For violations involving an insurance company that is licensed to do business in Kansas state, the insurance commissioner has the authority to bring to action provisions necessary for the breach in security.

**Covered Information:** Personal information refers to a customer's first name and last name or first initial and last name along with any of the following elements relating to the customer:

- Social security number
- Driver's license or state identification number
- Credit card or Debit card number
- Financial account number by itself or in combination with password, security or access code.

### Penalties:

The attorney general is in charge of imposing action if there are any violations of the code in the State of Kansas, except in the case of insurance companies who have a lawful license to do business in Kansas. For all other entities, the attorney general will deem what action (in equity or law) is appropriate.

The insurance commissioner is responsible for enforcing any actions on any violations committed by a state-licensed insurance company.

### Special Statutes for Certain Data Types:

None

### Data Breaches in Kansas:

- [Kansas data breach exposes millions of Social Security numbers](#) - Hackers gained access to over 5.5 million Social Security numbers in ten states by breaching a data system at the Kansas Department of Commerce. The department is required to pay for the credit monitoring of the victims whose sensitive data was exposed.
- [Kansas Department for Aging and Disability Services email reveals personal medical data](#) - An email sent by a KDADS employee contained an attachment which included names, addresses, DoBs, Social Security numbers, Medicaid data and other information. Banking, driver's license and credit card data was not included.

### Pending Data Breach Legislation in Kansas:

[H.B. 2359](#) Relating to the creation of the Kansas IT enterprise agency.

## Kentucky

**Reference:** KRS § [365.732](#), KRS §§ [61.931 to 61.934](#)

### Summary:

A security breach in the state of Kentucky is defined as acquiring, distributing, disclosing, manipulating, destroying or releasing unredacted or unencrypted data that is believed to have compromised the integrity, privacy or security of that data by a person, a business, an agency (branch of government in the Commonwealth of Kentucky, corporations, public school districts, universities and more) or by a non-affiliated third party (has a contract with an agency, a defined above).

This does not include the acquisition of data by an agent, employee or non-affiliated third party of the agency who use the data for the purpose of the agency only and it is not used in an unauthorized manner.

### Notification Requirements:

Any individual or business who conducts business in the state of Kentucky is liable to inform Kentucky residents if their unencrypted information has been breached without any unreasonable delay, as soon as they discover or are notified about the breach.

Any business or individual who maintains electronic data that has suffered a breach is liable to contact the owner or licensee of that data. If a law enforcement agency determines that a criminal investigation may be compromised by the breach, the notification may be delayed.

### To Individuals:

Notification may be provided in the form of a written notice or electronic notice (subject to stipulations). Substitute notification can be made if the cost of notification exceeds \$250,000 or the number of residents that need to be notified exceed 500,000, or the person or business does not have enough contact information for the affected residents.

Substitute notifications can be made in the form of a prominent notice on the website of the person or business or sending the notification out via state-wide media platforms.

### To Regulators:

If more than 1,000 residents have been affected by the breach, the person or business is liable to inform credit bureaus and consumer reporting agencies of the content, timing and distribution of the notifications, without any unreasonable delay.

**Covered Information:** Personal information including a resident's first name and last name, or first initial and last name, a personal identifying mark, a biometric image or genetic print along with one or more of the data elements below:

- Bank account number
- Credit card or debit card number (along with security or access codes, passwords and PIN that could be used to access the account)
- Social Security number or taxpayer identification number (which includes a SSN)
- Driver's license or state identification card number
- Individual identification number

- Passport number or any other unique identification number issued by the Federal government
- Identifying health information (except for education records)

**Penalties:**

None

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Kentucky:**

- [Protected health information disclosed by breaches in 2 Kentucky hospitals](#) - Medical data of 24,600 patients was exposed in a data breach at a psychiatric hospital in Louisville. The second breach occurred at a Medical Center in Bowling Green where a hard drive was deemed to be missing with patient data of over 5000 individuals.
- [Financial information exposed at Applebee's](#) - Applebee's revealed a data breach in March 2018, that may have disclosed credit and debit card information. Cyber security forensic firms were called in to investigate.

**Pending Data Breach Legislation in Kentucky:**

[H.B. 188](#) relates to a free security freeze for a protected person notified of a security breach. Also requires consumer reporting agencies to encrypt computerized data in consumer reports and files and facilitates requests for security freezes by the consumer reporting agency.

[S.B. 33](#) is related to revising provisions for the security of personally identifying information. Provides a security freeze for protected individuals who have been notified of a breach.

## Louisiana

**Reference:** La. Rev. Stat. §§ [51:3071 et seq.](#)

### Summary:

Defined as a breach in system security that results in or is believed to have resulted in an unlawful acquisition of personal electronic data maintained by an individual, corporation or government agency, that compromises the integrity, security and confidentiality of the data.

Acquiring of the personal information by an employee or an agent of the individual, corporation or government agency is seen to be in good faith, and not considered a breach of security, provided that the personal computerized data is not misused or disclosed in an unauthorized manner.

### Notification Requirements:

Any individual or business that is running a business in Louisiana and owns or licenses personal electronic data and believes or has reason to believe that a breach of security has occurred, needs to inform all affected Louisiana residents, without unreasonable delay.

Any individual, corporation or government agency that does not own personal data but maintains it, needs to promptly inform the owner or licensee of that data once they believe or have reason to believe that the data was compromised in an unauthorized manner.

Required measures also need to be taken to determine the impact of the breach and contain it to a reasonable extent. If it is determined by a law enforcement agency that the notice would obstruct a criminal investigation, then the notification can be delayed until it is established that the notice will no longer compromise the investigation.

### To Individuals:

Affected residents in the state of Louisiana may be notified by mailing a written notification, or an electronic notice (as per stipulations in 15 USC 7001).

Substitute notification can be sent if the individual, business or government agency determines that the cost of notifying residents exceeds \$250,000 or over 500,000 affected people need to be notified, or if enough contact data is not available for the affected residents.

Substitute notifications need to be emailed (when an email address is available), posted obviously on the website of the individual, business or agency, and broadcasted across the state via media outlets.

### To Regulators:

Notification of the security breach must also be sent simultaneously in writing, to the Louisiana attorney general's office at the Consumer Protection Section. The notice must contain details of the breach and include the names of all affected residents in Louisiana.

**Covered Information:** Personal information includes the unencrypted and unredacted Louisiana resident's first name (or first initial) and last name combined with 1 or more of the data elements below:

- Social security number
- Driver's license number



- Bank/financial account number
- Credit/debit card number (with necessary codes or passwords to gain access to the financial account)

#### **Penalties:**

If an individual, business or agency fails to provide timely notification to the attorney general (within 10 days of sending the notification to affected Louisiana residents) they may face a fine of not more than \$5,000 for each violation. Each day the notification is not received will be chargeable. The individual, business or agency may also face civil action to recuperate damages for failing to notify affected Louisiana residents in a timely fashion.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Louisiana:**

- [Medicaid data breach affects 13,000 Louisiana Residents](#) - Unauthorized employee access revealed personal information such as names, ID numbers, addresses, phone numbers and more for over 13,000 Medicaid recipients.
- [Louisiana Department of Children and Family Services suspends office and area manager for not discarding personal data](#) - Dozens of personal document copies containing bank records, social security cards, birth certificates and more were found in a trash can when they should've been properly shredded. Two employees were suspended.

#### **Pending Data Breach Legislation in Louisiana:**

[S.B. 361](#) is pending legislation relating to protecting electronic data that consists of personal information and requires notification in the event of a data breach.

## Maine

**Reference:** Me. Rev. Stat. tit. 10 § [1346 et seq.](#)

**Summary:** An unauthorized acquisition, use or disclosure of an individual's electronic data that includes personally identifying information that compromises the integrity, security and confidentiality of the personal data maintained by a person, corporation, LLC, estate, partnership or any other entity, including Maine government agencies and departments and private educational institutions such as colleges and universities.

Acquisition in good faith of the personal data by an employee or an agent of a person or entity is not considered as a breach of security if the personal data is not subject to unlawful use or unauthorized disclosure.

### **Notification Requirements:**

If a person, entity or broker (who collects, assembles and transmits personal data to non-affiliated third parties for a fee), discovers or is notified of a breach in security are liable in good faith to conduct an investigation on the breach and if they have reason to believe that a breach in security has occurred, need to inform affected residents in the state of Maine that their information has been compromised, without any unreasonable delay.

A third party that maintains the personal data on behalf of a person or entity, but does not own it, shall inform the person or entity of a security breach if they believe or have reason to believe that a breach in security has occurred.

If a law enforcement agency determines that the notification will not impede a criminal investigation then the notification has to be made in 7 days.

### **To Individuals:**

Notification to Maine residents can be made in the form of a written notice or electronic notice (subject to US Code law). A substitute notice may be provided in the event that the cost of notification exceeds \$5,000, or the number of state residents affected are over 1,000 people or the person or entity does not have adequate contact data for the affected Maine residents.

Substitute notifications must be made by email (if an email address is available), and by prominently posting the notification on the website of the person or entity and by broadcasting the notice to media outlets across the state of Maine.

### **To Regulators:**

If a security breach has affected more than 1000 people at one time, the person or entity needs to inform nationwide consumer reporting agencies the date, approximate number of individuals affected by the breach and the timing of the notification to affected individuals.

**Covered Information:** In the state of Maine, personal information covered includes the first name (or first initial) and last name combined with 1 or more of the identifying pieces of data below, when either the name or any elements of the data are unredacted and unencrypted:

- Social security number
- Driver's license number or an identification number in the state of Maine

- Bank account number
- Credit or debit card number, if such a number can be used without passwords/access codes
- Personal identification numbers, account passwords or any other access codes

#### **Penalties:**

State regulators of the Dept. of Professional and Financial Regulation are responsible for enforcing any action on entities that are licensed or regulated under them. For all other persons and entities, the Attorney General is liable to take action.

Violation fines fall under civil violations and are not more than \$500 for each violation, for a maximum of \$2,500 per day the person or entity is found to be in violation. They are also subject to equitable relief.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Maine:**

- [2,100 foster care benefit residents affected by security breach](#) - The Maine Office of IT disclosed that the names, SSNs and addresses of individuals including legal guardians and children, involved with the foster care services at the Department of Health and Human Services were temporarily disclosed on a 3rd-party website. Free credit monitoring services were offered to the affected residents.

#### **Pending Data Breach Legislation in Maine:**

None

## Maryland

**Reference:** [Md. Code](#) Com. Law §§ 14-3501 *et seq.*, Md. State Govt. Code §§ 10-1301 to -1308

**Summary:** An unauthorized acquisition of electronic data that compromises the integrity, security and privacy of the data maintained by a business.

This does not include any acquisitions in good faith of the personal data by an agent or employee for the business, under the condition that the data is not used or disclosed in an unauthorized or unlawful manner.

### **Notification Requirements:**

Any business operating or licensing electronic data in the state of Maryland is liable to conduct a prompt investigation in good faith, when it determines that a security breach has occurred and the personally identifying information can or will be compromised. In the likelihood that this is found to be the case, the business is liable to notify, without unreasonable delay the Attorney General (and no later than 45 days), all affected residents in the state of Maryland.

If the event that after the investigation the business determines that residents' information will not be subject to unauthorized disclosure, the records of the investigation and determination need to be maintained for 3 years.

Any business maintaining personal data for individuals residing in Maryland, but not owning or licensing it, is responsible for contacting the owner or licensee as soon as they discover or are notified of a breach. They are also liable to share any information in respect to the breach with the owner/licensor of that data.

A delay in notification is only applicable if a law enforcement agency determines that the notice will compromise homeland security or a criminal investigation. If this is determined to not be the case then the notification needs to be given in no later than 30 days.

### **To Individuals:**

Businesses owning, licensing or maintaining personal data need to notify individuals of a security breach by mailing a written notice to the most recent address, by telephone, or by sending an email (as long as the individual is in consent of receiving email notifications from the business).

A substitute notice may be provided if the business shows that the cost of the notifications will exceed \$ 100,000 or the number of affected Maryland individuals exceeds 175,000 people, or not enough contact data is available for the residents.

The substitute notice will be provided in the form of an email (if one is available), and by posting the notice prominently on the business's website and also by broadcasting the notice through media outlets throughout the state of Maryland.

Businesses who own or license personal data in Maryland are also responsible to include in the contents of the notice; what information was disclosed in the breach, include contact information, address and possibly a toll-free number of the business and of major consumer reporting agencies, the Federal Trade Commission and The Office of the Attorney General, including next steps to avoid theft of identity.

### **To Regulators:**

If the breach involves 1000 or more Maryland residents, the business shall inform consumer reporting agencies nationwide, without unreasonable delay on the content, timing and distribution of the notices. The names or any personal data pertaining to affected residents does not need to be included.

**Covered Information:** Personal data includes any resident of Maryland's first and last name, or first initial and last name combined with any of the data elements below, unless the data is encrypted, rendered unusable or redacted:

- Social security number
- Driver's license number
- Financial account number including credit/debit card information (with access codes and passwords)
- Individual Taxpayer ID number or state identification number
- Passport number
- Health information, insurance, HIPAA, and medical history data
- Biometric data (fingerprint, retina image, voice print etc.)
- User account information with security questions

**Penalties:**

Any business found in violation is subject to penalties and enforcement of the law as per the Consumer Protection Act.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Maryland:**

- [City employee data stolen to file fraudulent tax returns](#) - The City of Baltimore involved federal and state investigators to determine the cause of the potential breach. Free credit monitoring services were offered to employees.

**Pending Data Breach Legislation in Maryland:**

None

## Massachusetts

**Reference:** Mass. Gen. Laws § [93H-1 et seq.](#)

**Summary:** A breach of security in the state of Massachusetts is defined as the unauthorized access of unencrypted data or encrypted data, provided that the key to access the data is available, maintained by a person (person, corporation or legal entity) or agency (a government department, bureau, office etc.) that compromises the confidentiality, security or integrity of the personally identifying data.

An acquisition in good faith by a person or agency or the employee or agent of a person or agency is not considered a breach of security unless the data is subject to unauthorized release or disclosure.

### **Notification Requirements:**

Any person or agency that stores or maintains the data needs to inform, without unreasonable delay, the owner or licensor of the data if they know or have reason to believe that a breach of security has occurred.

Notification may be delayed in the event that a law enforcement agency believes that the notice may obstruct a criminal investigation, however the attorney general needs to be informed in writing if this is the case. Persons and agencies are also required to fully cooperate with law enforcement agencies and share any pertinent information regarding the breach.

### **To Individuals:**

Notification to individuals may be given in the form of a written notice or an electronic notice (according to certain provisions of the United States Code).

A substitute notice may be provided in the case a person or agency does not have enough contact information for affected residents or can show that the cost of providing the notifications goes beyond \$250,000, or that the number of Massachusetts residents needing to be notified goes over 500,000 residents.

The substitute notifications can be provided to affected Massachusetts residents by email (provided an email address is available), through an obvious posting on the website of the person or agency, and through a media broadcast or publication throughout the state.

### **To Regulators:**

Along with notifying affected Massachusetts residents, persons and agencies are also liable to inform the attorney general as well as the office of consumer affairs and business regulation, without unreasonable delay as soon as they discover or are notified about the breach.

**Covered Information:** Personal information which includes a person's first and last name, or first initial and last name along with one or more of the data elements relating to a Massachusetts resident below:

- Social Security number
- Driver's license number or identification card number for the state of Massachusetts
- Bank account number
- Credit card or debit card number (which includes or does not include any access or security codes, PIN or password that would access to that resident's account)

### Penalties:

The attorney general may take action in the form of relief or what may be deemed appropriate, against an entity found in violation of the code.

### Special Statutes for Certain Data Types:

None

### Data Breaches in Massachusetts:

- [Equifax data breach affects more than 3.3 million Massachusetts residents](#) - More than half of the Massachusetts state's population were affected by a massive data breach thanks to Equifax.
- [Over 14,000 state residents affected by a security breach by Intercontinental Hotels Group](#) - In April 2017, this major security breach in Massachusetts revealed financial data such as credit and debit card numbers of Mass. residents.

### Pending Data Breach Legislation in Massachusetts:

[H.B. 2814](#) would appoint a special cybersecurity commission in the Commonwealth to investigate security threats and breaches.

[H.B. 134](#) relates to discarding fees concerning security freezes and disclosing credit reports from consumers.

[S.B. 95](#) is related to the protection of biometric data.

[S.B. 149](#) relates to the confidentiality of personally identifying financial information.

[H.B. 4910](#) relates to facilitating a policy for database security breaches for state agencies.

[H.B. 4983](#) revises notice of security breach requirements, requires public access.

## Michigan

**Reference:** Mich. Comp. Laws §§ [445.63](#), [445.72](#)

**Summary:** In Michigan, a breach of security of a database is defined as the illegal acquisition or authorization of personal information. The personal information access could be of that of a single or of multiple individuals that is maintained by a person or an agency.

The breach of data security is not applicable if the employee or agency has not misused the personal information nor has disclosed it to unauthorized personnel. Additionally, the access to data is not termed as a security breach if the access was for the activities of the agency and was done in good faith by the employee accessing the data.

### **Notification Requirements:**

An agency or person needs to provide notice regarding the security breach without unreasonable delay. A delay in notification shall be allowed if it is necessary for the agency to restore the integrity of the database or determine the extent to which the breach will affect Michigan residents. In either case the agency must notify immediately after the scope of breach has been identified and integrity of the database restored.

The notification can also be delayed if a law enforcement agency concludes that providing a notice does hinder a civil or criminal investigation or expose national or homeland security.

### **To Individuals:**

The agency needs to notify the Michigan resident either by written mail or electronic mail if that is the preferred method and the most current mode of communication by the resident. Additionally, the agency is allowed to communicate via email if that is how the agency conducts its transactions with the resident.

The resident can also be contacted via telephone if the message is not a recorded message and the agency has not been able to have a personal conversation between the individual within 3 business days of written communication.

If the cost of sending the notification of breach exceeds \$250,000 or if the agency has to provide notice to more than 500,000 Michigan residents it can send a substitute notice. A substitute notice could be an electronic notification, a notice on the agency website and a notification to state-wide media.

### **To Regulators:**

The person or agency also needs to provide a notice to other consumer reporting agencies without unreasonable delay. This is not applicable if the agency is required to send a notice to fewer than 1000 residents of the state.

**Covered Information:** Covered information includes the first name and last name or first initial and last name along with one of the following data elements:

- Social security number
- Driver license number or Personal identification card number of the state
- Financial account number, demand deposit, credit card or debit card number in combination with a password, access code or security code that would allow access to the financial account of a Michigan state resident



### **Penalties:**

A misdemeanor that fails to provide a notice of security breach is punishable by law. For a first violation it includes a fine of not more than \$250 or imprisonment of not more than 93 days or both. For a second violation it could include a fine of not more than \$500 or imprisonment of not more than 93 days or both. For a third violation it could include a fine of not more than \$750 or imprisonment of 93 days or both.

For multiple violations arising from the same security breach the penalty shall not exceed \$750,000. A prosecuting attorney or an attorney general may take necessary action to recover the civil fine.

### **Special Statutes for Certain Data Types:**

None

### **Data Breaches in Michigan:**

- [State of Michigan's Computer System](#) – In February 2017, the state computer system reported a glitch that exposed the personal information of residents.

### **Pending Data Breach Legislation in Michigan:**

[H.B. 5094](#) is a pending act for reporting agencies to place, remove and authorize security freezes for consumers under certain circumstances.

## Minnesota

**Reference:** Minn. Stat. §§ [325E.61](#), [325E.64](#)

**Summary:** In Minnesota, breach of security refers to the unauthorized access of electronic data maintained by a person or business that can compromise the integrity, confidentiality and security of that computerized data.

Acquisition of data by an employee or agent of the person or business to be used by the person or business is not considered to be a breach of security, unless the information is subject to disclosure in an unlawful manner.

Breach of security for access devices deems any person or business in Minnesota accepting a credit or debit card for transaction purposes, shall not retain the security code, PIN number or magnetic stripe data for more than 48 hours.

### **Notification Requirements:**

A person or business conducting business in the state of Minnesota that owns or licenses personal data shall notify Minnesota state residents when a breach is discovered or they are notified of the breach and believes or has reason to believe that the unencrypted personally identifying information was compromised, without unreasonable delay.

Any business or person maintaining personal data (but not owning it), needs to inform the owner/licensee of that data immediately upon discovery or being notified of the breach.

The notification may only be delayed if a law enforcement agency establishes that the notification will compromise a criminal investigation.

### **To Individuals:**

Notification may be provided in writing by mailing the notification to the most recent address or by electronic notice (subject to stipulation).

A substitute notice may only be provided if the person or business is able to determine that the cost of sending the notifications would surpass \$250,000 in costs, or the number of affected Minnesota residents exceeds more than 500,000 individuals.

Substitute notifications need to be made in the form of email notices, posting an eye-catching notice on the website of the person or business, and by notifying statewide media outlets in the state of Minnesota.

Apart from providing substitute notifications, if a person or business maintains their own security policies and notification procedures that are in compliance with the notification requirements of the security code, they can use that notification procedure to inform affected residents in the event of a security breach.

### **To Regulators:**

If a person or business determines that more than 500 residents have been affected by the security breach, they are also liable to notify, in a period of 48 hours, major consumer reporting agencies on the content of the notices sent along with when they were sent and how they were distributed.

**Covered Information:** Personal information refers to a Minnesota resident's first name (or first initial) and last name, combined with 1 or more of the data elements below, when the data is unencrypted, rendered unusable or the key to access secure encrypted data was also obtained:

- Social Security number
- Driver's license number / a Minnesota ID card number
- Financial account number
- Credit / debit card number (along with security codes, passwords or access codes that would allow access to that resident's financial data)

**Penalties:**

A person or business is considered to be in violation if they fail to disclose a security breach or retain any access card transaction data for more than 48 hours after the transaction has been authorized. The attorney general is responsible for enforcing penalties to violators of under section 8.31, additional duties of the attorney general.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Minnesota:**

- [Anthem security breach affects 300,000 Minnesota residents](#) - Health insurance company, Anthem, reported a massive data breach affecting 80 million nationwide, including revealing SSN and personally identifying data of Minnesota residents.

**Pending Data Breach Legislation in Minnesota:**

[H.B. 1507](#) relates to education. It establishes the Student Data Privacy Act and provides penalties.

[H.F. 3480](#) is related to providing regulations with consumer reports and dispute resolutions, including credit monitoring services.

[S.F. 1811](#) is pending legislation relating to providing exceptions and authorizing security freezes.

## Mississippi

**Reference:** [Miss. Code](#) § 75-24-29

**Summary:** Breach of security is defined as the unlawful acquisition of unencrypted or unreadable computerized data, including databases, electronic and media files which contain personal data of any Mississippi state resident owned, licensed or maintained by a person conducting business in the state.

### Notification Requirements:

Any person conducting business in the state of Mississippi is required to immediately disclose a breach of security to all residents affected in Mississippi, once they complete an investigation to determine the scope and impact of the breach, identify affected residents and restore the data system breached.

If the investigation deems that the breach will not compromise any personally identifying data, a notification will not be required.

Any person maintaining electronic personal data but not owning or licensing it, is required to notify the owner or licensee of the personal data as soon as the breach was discovered or they believe or have reason to believe that the data was used in an unlawful manner.

Notification can be delayed in the event that the law enforcement agency establishes that the notice may hamper national security or a criminal investigation.

### To Individuals:

Notification to individuals can be made in writing, by telephone or by email (if email is the primary way the person communicated with the resident or other provisions subject to stipulations).

A substitute notice may be provided if the person is able to demonstrate that the cost of providing the notifications will exceed an amount of \$5,000 or the number of Mississippi residents needing to be notified exceed 5,000 individuals, or the person has inadequate contact information for the affected residents.

Substitute notifications can be made in the form of email (if the email address is available), posting the notice in a prominent fashion on the website of the person and notifying media outlets such as radio, television stations, newspapers across the state of Mississippi.

### To Regulators:

None

**Covered Information:** Personal information includes the first name and last name, or first initial and last name including one or more of the personally identifying elements below:

- Social security number
- Driver's license or state identification number
- Bank account number
- Credit or debit card number including security codes, passwords and any access codes that would allow access to that individual's account

### Penalties:



All violations and failure to comply are constituted under unfair trade practice and are enforced by the Attorney General.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Mississippi:**

- [Testing vendor exposed data from 663 students](#) - Mississippi education authorities revealed a data breach by Questar Assessment, that administers standardized math, English and arts tests. No social security numbers or addresses were released. No penalties reported.
- [Mississippi Centers for Disease Control and Prevention client health information compromised](#) - Personal health information for the Centers for Disease Control and Prevention was leaked to a government contractor. The Mississippi State Department of Health will offer free credit monitoring protection for 1 year to clients whose names, lab results, social security numbers and other data were exposed.

**Pending Data Breach Legislation in Mississippi:**

None

## Missouri

**Reference:** Mo. Rev. Stat. § [407.1500](#)

**Summary:** In Missouri, a security breach is defined as unauthorized access to personal information that is maintained electronically and has the confidential information of the resident. Acquisition of personal information in good faith and for a legitimate purpose by an agent does not constitute as breach of security.

### Notification Requirements:

A person or agency that is licensed to have personal information of a Missouri resident needs to provide notice to the affected consumer without unreasonable delay as per the requirement of the law enforcement agency. The notification must be consistent with the needs of the data system to maintain and restore the reasonable confidentiality, security and integrity of the data system.

The notification could be delayed if a law enforcement agency mentions that it could risk national or homeland security or hinder a criminal investigation. Once the law enforcement agency has communicated to go ahead to send the notification it shall be sent without unreasonable delay.

A notification is not essential if after consultation and necessary investigation by relevant agencies of law enforcement, it is determined that the fraud or identity theft does not constitute a breach. This determination needs to be documented for five years.

### To Individuals:

The consumer shall be notified by a written notice or an electronic notice if the resident has provided a valid email address and has given consent to receive email notice. Notice by telephone is also acceptable if the consumer can be reached directly.

If the person or agency demonstrates that the expense of providing a notice exceeds \$100,000 or if the number of residents affected are greater than 150,000, a substitute notice can be sent. A substitute notice can also be sent if there is insufficient contact information or if the agency is not able to identify particular affected residents.

A substitute notice needs to be sent in the form of an email notice, a posting on the website of the person or agency and through major state-wide media.

### To Regulators:

If a person or agency needs to provide notice to more than 1000 Missouri residents at a time, the person or agency also needs to inform the office of the attorney general without unreasonable delay regarding the security breach.

**Covered Information:** Covered information includes the first name and last name or first initial and last name in combination with any other data element such as:

- Social security number
- Driver's license number or a government issued unique identification number
- A debit card number, credit card number or a financial account number that can access the resident's financial account along with it a password, security or access code
- Unique routing code or electronic identifier along with a password, security or access code that can be used to access the resident's financial account

- Health insurance information
- Medical information

**Penalties:**

The attorney general has the authority to take action to retrieve actual damages for a purposeful violation and can seek a civil penalty not exceeding \$150,000 for breach of data security of the system discovered in a particular investigation.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Missouri:**

- [BJC Healthcare](#) - In March 2018, BJC healthcare reported an unsecured server that could have given access to patients' information such as insurance cards, treatment records, social security number and other personal information.
- [Missouri Department of Mental Health sends 1000 names to incorrect address](#) - The mental health department notified a thousand people whose names were incorrectly mailed to a wrong address. No penalties reported.

**Pending Data Breach Legislation in Missouri:**

None

## Montana

**Reference:** Mont. Code §§ [2-6-1501 to -1503](#), [30-14-1701 et seq.](#), [33-19-321](#)

**Summary:** In the state of Montana, a breach of system security is defined as the unauthorized acquisition of electronic data that significantly compromises the personal data's integrity, privacy and security maintained by an individual or a business and creates or is reasonably believed to have created damage and loss to a resident in the state of Montana.

### **Notification Requirements:**

A business or individual needs to notify, without unreasonable delay, affected residents in Montana and take any necessary measures to restore the integrity of the system that was breached in a reasonable manner. They must also comply with the legal requirements of law enforcement.

The notification may be delayed only if a law enforcement agency deems that it will disrupt or slow a criminal investigation. However, once the agency establishes that the investigation will not be compromised, the notification must be made without delay.

### **To Individuals:**

Notification to Montana residents must be made in writing, by telephone or through electronic notice (as per conditions set in 15 U.S.C. 7001).

A substitute notice may also be sent if the person or business does not have adequate contact data for the affected residents or is able to show that the cost of sending the notifications will go over \$250,000 or the number of people to be notified exceeds 500,000.

Substitute notifications must be sent via email, posting a prominent notice on the business or individual's website and broadcasting the notice to media outlets across the state.

### **To Regulators:**

An individual or business is also responsible for simultaneously submitting an electronic copy of the notification to the attorney general at the Office of Consumer Protection (OCP), also providing a statement with the timing of the notification and how it was distributed (by mail, telephone, email etc.).

If the notification was sent to more than one Montana resident, only one copy needs to be sent to the OCP indicating the number of residents in Montana who received the notice.

Entities involved in the insurance business do not need to send a copy of the notification to the attorney general's office but may be required to send a notification to the Commissioner of Insurance.

**Covered Information:** Unencrypted data comprising of a person's first and last name, or first initial and last name along with any of the data elements listed below:

- Social security number
- State ID, Tribal ID or driver's license number
- Bank account number
- Debit or credit card number long with a password/security/access code that would allow access to that individual's account
- Medical record data



- Taxpayer ID / Unique ID issued by the US internal revenue service

**Penalties:**

In cases where the department has reason to believe that an individual or business is in violation, the department may enforce action on behalf of the state which may include a permanent or short-term injunction or restraining order.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Montana:**

- [Montana hacking breach affects 1.3 million](#) - A breach at the Dept. of Public Health and Human Services may have compromised names, SSN, addresses and health data. Free credit monitoring services were offered for a year to affected residents.
- [Data security breach exposes personal information of nearly 1000 Montana residents](#) - Billings Clinic sent letters to affected residents after discovery of its email system being compromised. Patient names, phone numbers and pending amounts to Billings Clinic's Atrium Pharmacy were exposed. No penalties reported.

**Pending Data Breach Legislation in Montana:**

None

## Nebraska

**Reference:** Neb. Rev. Stat. §§ [87-801 et seq.](#)

**Summary:** A breach of system security refers to the unauthorized acquisition of electronic data that has not been encrypted and compromises the integrity, security and privacy of that data which is maintained by an individual (a natural person), or a commercial entity (corporation, LLC, LLP, government department or agency, trust, estate and more).

An agent or employee of the individual or commercial entity accessing the information for the purposes of the agent or commercial entity is seen as acquisition in good faith and not considered as a breach in security, unless the personal information is subject to unlawful disclosure.

Further, acquiring the information for the purposes of a subpoena, court order or search warrant is not considered as a breach of system security.

### **Notification Requirements:**

Any individual or commercial entity conducting business in the state of Nebraska and owns or licenses personally identifying electronic data of Nebraska residents needs to conduct an immediate investigation, in good faith, to ascertain the details of the breach and if the personal information has been disclosed in an unauthorized manner.

If the individual or commercial entity has reason to believe that the information has been or can potentially be disclosed needs to, without unreasonable delay, notify affected Nebraska residents. They also need to take necessary steps to restore the integrity of the data system breached.

Individuals or entities that maintain personal information are liable to notify the owner or licensee of the personal data, without unreasonable delay, as soon as they become aware of or are notified of the breach.

Notification may be delayed if a law enforcement agency determines that the notice to Nebraska residents will encumber a criminal investigation.

### **To Individuals:**

Notification to Nebraska residents has to be made in the form of a written notice, telephone notice or electronic notice (subject to stipulations). A substitute notice may be provided but only if the individual or entity can demonstrate that the cost of providing notification exceeds \$75,000 or over 100,000 affected Nebraska residents need to be notified.

Substitute notification can be provided by email, a prominent posting on individual or entity's website and by broadcasting the notice to media platforms across the state.

If the individual or commercial entity has 10 employees or less and shows that the cost of notifications will surpass \$10,000, a substitute notification can be sent in the form of email, paid quarter-page ads in a local newspaper that falls within their area, every week for 3 consecutive weeks, and posting the notice conspicuously on the website of the individual or entity and notifying media outlets in their local area.

### **To Regulators:**

When an individual or entity determines that a notification for breach of security is required, they will also notify the Attorney General, no later than the timing of the notification to Nebraska residents.

**Covered Information:** Personal information for Nebraska residents, which includes the first name, or first initial and last name along with 1 or more of the unencrypted, unreadable and unredacted data elements below:

- Social security number
- Driver's license number or state identification card number
- Financial account number
- Credit / debit card number (along with a password, access or security code that would allow access to the resident's account)
- Unique electronic ID number or routing code (along with a required password, security or access code)
- Personally identifying biometric data, (iris/retina image, fingerprint or voice print)
- Login data combined with security information to access the account

**Penalties:**

Enforced by the Attorney General, violators may face action in the form of subpoenas and the Attorney General may seek and recuperate financial damages for each Nebraska resident whose personal information was compromised and is affected by a violation.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Nebraska:**

- [University of Nebraska data breach exposes data of 650,000 students](#) - This massive data breach leaked personal information including Social Security numbers, address and course grades.

**Pending Data Breach Legislation in Nebraska:**

None

## Nevada

**Reference:** Nev. Rev. Stat. §§ [603A.010 et seq.](#), [242.183](#)

**Summary:** Breach of data security in Nevada refers to the unlawful acquisition of electronic data that compromises the confidentiality, integrity and security of the personal data maintained by a data collector such as a corporation, government agency, financial or educational institution or any other type of business that collects, deals with or distributes private personal data.

This does not include acquisitions in good faith by an employee or agent of the data collector, for the purposes of the data collector as long as the data is not disclosed in an unauthorized manner.

### Notification Requirements:

A data collector that either owns/licenses personally identifying electronic data needs to inform affected residents in the State of Nevada when they discover or are notified of a security breach without an unreasonable delay. Necessary measures also need to be taken to reasonably restore the integrity of the system breached.

A data collector that maintains, but does not own/license the data, is accountable to notify, without unreasonable delay the owner or licensee of the data as soon as a breach is discovered or are notified of the breach and believe or have reason to believe that personal data was compromised.

Only if a law enforcement agency determines that the notification will slow or disrupt a criminal investigation, the notification can be delayed.

### To Individuals:

Notification needs to be provided in writing or by electronic means (as per the provisions set under the Electronic Signatures in Global and National Commerce Act). Substitute notification may only be provided if the data collector is able to show that the cost of sending notices will exceed \$250,000, the number of affected Nevada residents needing to be notified surpasses 500,000 people or the data collector does not have enough contact data for each resident.

Substitute notifications can be made in the form of email, posting the notification noticeably on the data collector's website and notifying media outlets in the state of Nevada.

### To Regulators:

If the notifications needing to be sent exceed 1000 people, the data collector needs to notify consumer reporting agencies on the timing, content and distribution of the notifications, without unreasonable delay.

**Covered Information:** Personal information is defined as an individual's first name/first initial and last name combined with 1 or more of the unencrypted data elements below:

- Social security number
- Driver's license number / authorization or identification card number
- Bank account number
- Credit/debit card number with necessary password, security or access code to gain access to the financial account.

- Health insurance or medical ID number
- Unique login information (username and password) with any security questions or access codes which allow access to the account

Last 4-digits of SSN, driver's license or authorization and identification card are not included.

#### **Penalties:**

Penalties can be in the form of civil action, restitution or injunction. A data collector can take action and collect damages in the form of lawyer fees, notification costs, punitive damages and more, against the person that obtained the data in an unauthorized manner.

The court can also order the unauthorized person to pay restitution for notification costs to the data collector. The Attorney General or county district attorney has the right to take action in the form of a short-term or permanent injunction against the violators.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Nevada:**

- [Nationwide insurance pays over \\$100,000 to Nevada data breach residents](#) - Nevada along with 31 other states filed a lawsuit against Nationwide Mutual Insurance Co., for a 2012 data breach which exposed Social security numbers, credit scores and driver's license information, and cost the insurance company \$5.5 million.

#### **Pending Data Breach Legislation in Nevada:**

None

## New Hampshire

**Reference:** N.H. Rev. Stat. §§ [359-C:19 et seq.](#)

**Summary:** An unauthorized acquisition of electronic personal information that compromises the privacy or security of that information maintained by an individual, corporation, LLC, agency, government entity or any other form of business.

Access by an employee or agent of the individual or business for the purposes of the individual or business is considered to be in good faith and not deemed as a breach in system security, as long as the personal data is not subject to be used or disclosed in an unauthorized fashion.

### Notification Requirements:

Any individual or business who conducts business in the state of New Hampshire and owns/licenses personal data needs to conduct a prompt investigation upon discovering a breach of security.

In the likelihood this determination shows that the personal data is compromised or can potentially be compromised, the individual or business is responsible to notify affected New Hampshire residents without unreasonable delay.

An individual or business maintaining personal data is responsible for notifying the owner/licensee of the data, as soon as they become aware of or are notified of the breach. Notification may be postponed only if a law enforcement agency determines the notice will compromise homeland or national security or hinder a criminal investigation.

### To Individuals:

Notification needs to be provided in writing, by telephone or by email (only if the individual/business communicated with residents prior to the breach by email).

A substitute notification may be provided if the individual or business does not have enough contact data for the affected residents or can establish that the cost of sending notifications exceeds \$5,000, or the number of affected New Hampshire residents to be sent the notices goes over 1000 people.

In that case substitute notifications can be sent in the form of email, prominently posting the notification on the website of the individual or business and distributing the notification via state-wide media.

### To Regulators:

Any individual or business conducting trade or commerce is responsible for notifying the regulatory official with authority over that trade or commerce. All other businesses and individuals are responsible for notifying the office of the attorney general in New Hampshire.

If more than 1000 New Hampshire residents have been affected by the breach, the individual or business is also required to notify major consumer reporting agencies.

**Covered Information:** Personal information of a New Hampshire resident's first name (or first initial) and last name combined with 1 or more of the unencrypted data elements below:

- Social security number
- Driver's license number
- Any other government ID number
- Financial account number
- Credit card or debit card number (combined with the requisite password, security and access code such as a PIN, that can provide access to a New Hampshire resident's account)

Personal data does not include public data in government records.

#### **Penalties:**

An individual or business that suffered damages can bring an action in court and demand an injunction and equitable relief for the violation. If the plaintiff wins the case, actual damages can be recovered. If the court deems the violation was willful, it can award three times, but not less than twice, the damage amount. The court can also award other costs such as attorney fees. The attorney general's office is responsible for enforcing action.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in New Hampshire:**

- [New Hampshire Department of Health and Human Services breach revealed data of 15,000 patients on social media](#) - A patient of a New Hampshire hospital hacked into the DHHS system and gained access to SSN, Medicaid information and addresses, which were later posted on social media. No penalties reported.

#### **Pending Data Breach Legislation in New Hampshire:**

[HB 1700](#) (LSR 2410) is legislation relating to placing a security freeze on an individual's credit. Passed and goes into effect 1-1-2019.

[SB 303](#) (LSR 2766) relates to placing a security freeze on an individual's credit report. Passed and goes into effect 1-1-2019.

## New Jersey

**Reference:** N.J. Stat. [§§ 56:8-161, 163, 165 – 166](#)

### State Agency Guidance Materials:

**Summary:** In the State of New Jersey, data breach legislation applies to all businesses and state entities operating in New Jersey, or; which through the course of their business obtain computerized personal information of residents of New Jersey.

Under New Jersey [data breach notification law](#), a breach is defined as unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

### Notification Requirements:

Once a business or public entity becomes aware of a data breach, they are required to notify in the first instance, without unreasonable delay, the Division of State Police in the Department of Law & Public Safety. Once the breach is being handled or investigated appropriately, determination will be made as to notification of individuals and regulatory bodies as follows.

#### To Individuals:

Notification to individuals whose personal information has been breached is to be made in the most expedient manner without reasonable delay. The caveat to this is that notification is not required if the business or public entity can establish that misuse of the information is not reasonably possible. Such determination must be made and kept in writing for five years. Further, if notification is required, notification will be delayed if it is determined by a Law Enforcement Agency that such notification could hinder a criminal or civil investigation. If this is the case, the Law Enforcement Agency can notify the business of the appropriate timing of notification following the investigation.

#### To Regulators:

As mentioned previously, the first notification required is to the Division of State Police in the Department of Law & Public Safety. Further, if more than 1000 persons at one time are affected by this data breach, the business or public entity must also notify all consumer reporting agencies responsible for compiling or maintaining files on national databases. In this instance the timing, distribution and content of notifications will be governed by the Federal Fair Credit Reporting Act. The Division of State Police may also advise of any other regulatory bodies that must be notified due the nature of a data breach.

**Covered Information:** Under this legislation, covered information includes: The first name or first initial and last name of a person that is also linked to one or more of the following:

- Social Security Number
- Driver's License number
- State ID number



- Account number, credit card or debit card number; if this is also linked with any required security code, access code or a password that would allow unauthorized access to the person's financial account.

#### **Penalties:**

Penalties for data breaches in New Jersey can include civil action, substantial fines paid to the state, requirement to destroy data, and to implement Corrective Action Plans including cyber-security reforms.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in New Jersey:**

The Department of Law & Public Safety - Office of the Attorney General releases statistics relating to data breaches in New Jersey through the [NJ Cybersecurity & Communications Integration Cell](#).

- [VIZIO to Pay \\$2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent](#) - A Smart TV manufacturer and their subsidiary VIZIO Inscape Services were found to be in breach of data laws in February 2017. The company had unlawfully tracked, collected and sold customers viewing data to marketing companies and data brokers. As a result of the breach VIZIO was required to pay \$2.2 million to the state and VIZIO Inscape were required to pay \$915,940 in civil penalties and \$84,060 in legal and investigative costs. They were also required to destroy consumer viewing data prior to an agreed date and subsequently clearly disclose to consumers what data they collect through their Smart TV's and gain express permission prior to doing so. Further they were required to implement an ongoing privacy program to comprehensively protect customers from future breaches.
- [NJ Releases Annual Statistics on Data Breaches for the First Time](#) - Horizon Medical Insurers were found to be in breach of the New Jersey Consumer Fraud Act, Federal Health Insurance Portability Accountability Act (updated to Health Information Technology for Economic & Clinical Health Act). This was due to two laptops being stolen from the Insurer's Headquarters which were holding unencrypted personal data of almost 690,000 New Jersey policy holders. As a result of the breach they were required to pay the State \$1.1 million and to implement a Corrective Action Plan.
- [NJ Releases Annual Statistics on Data Breaches for the First Time](#) - Target Incorp. (Target) was involved in a multistate investigation that included New Jersey on the Executive Committee. The basis of the investigation was a data breach resulting in compromised payment card data of more than 41 million customers nationwide. As a result of the multistate investigation Target was required to pay \$680,411 to New Jersey as well as adopt a range of cyber-security reforms including an Information Security Program to prevent future data breaches.

#### **Pending Data Breach Legislation in New Jersey:**

As outlined in the National Congress of State Legislatures, New Jersey currently has a number of [pending data laws for 2018](#).

- [A.B. 2427](#) prohibits consumer reporting agencies from charging certain fees and including certain provisions in contracts with consumers.
- [A.B. 1360](#) requires certain notifications and free credit reports for customers following breach of security of personal information within business or public entity.
- [A.B. 3043](#) requires consumer reporting agencies to increase protection of consumers' personal information.
- [A.B. 3245](#) requires disclosure of breach of security of online account.
- [A.B. 3541](#) revises requirements for disclosure of a breach of security of certain computerized records containing personal information.
- **S.B. 52** requires disclosure of breach of security of online account.
- [S.B. 1524](#) revises requirements for disclosure of a breach of security of certain computerized records containing personal information.
- [S.B. 1850](#) requires consumer reporting agencies to increase protection of consumers' personal information.

## New Mexico

**Reference:** N.M. [Stat. §§ 57-12C-1 – 57-12C-12](#)

### State Agency Guidance Materials:

**Summary:** The data breach notification law of New Mexico, tabled as [H.B.15](#), was signed on April 6, 2017 and went into effect on June 17, 2017. New Mexico was the 48th state to enact legislation making it mandatory for individuals to be contacted when their personal identifying information is compromised in a data breach.

The New Mexico legislation defines a security breach as the unauthorized procurement of unencrypted computerized data or encrypted computerized data when the encryption code or key has also been compromised. Further, the data intrusion negatively impacts the privacy, integrity, or security of the Personal Identifying Information (PII) held by a person. Excluded from this is the good-faith acquisition of PII by employees or agents for legitimate business purposes.

### Notification Requirements:

#### To Individuals:

A security breach must be reported to each person affected as soon as possible after discovery and within 45 calendar days.

Notification must be made through the United States postal service or electronic notification if this is the usual method of communication used by the notifying party. A substitute notification method is permitted if the notifying party can demonstrate that using either of the methods outlined above would cost in excess of \$50,000 or the number of individuals to be notified exceeds 100,000, or there is insufficient contact information on file for a person. Acceptable substitute notification methods include the submission of written notification to the Attorney General's office and major news organizations in New Mexico, visible publication of the notice on the reporting organization's website, or the forwarding of an electronic notification to those individuals for whom the entity has a valid email address.

Should the authorized gatekeeper possessing or maintaining the compromised PII be a third-party, they must notify the rightful owner of the data within 45 calendar days.

However, if after an appropriate investigation by the gatekeeper responsible for the PII, it is ascertained the breach did not significantly expose the data to theft or identity fraud, notification is not deemed necessary.

Any individual subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996 is exempt from this legislation.

#### To Regulators:

Entities required to issue notification of a security breach to more than 1,000 New Mexico citizens are legally obligated to notify both the New Mexico Attorney General, and Consumer Reporting agencies within 45 calendar days of discovery.

**Covered Information:** Covered information pertains to a person's first name or initial and surname linked to one or more of the following:

- Social Security Number
- Driver's license or a State issued identification card number
- Biometric data
- Debit or credit card account numbers (combined with matching security, access codes or passwords)

**Penalties:** The Attorney General may file a court action when reasonable evidence exists to believe a violation of the Act has occurred. The court may levy a civil penalty of the greater of \$25,000 (twenty-five thousand dollars). In the event of failed notification, fines in the amount of \$10.00 (ten dollars) per violation to a maximum of \$150,000 (one-hundred-and fifty-thousand dollars).

**Special Statutes for Certain Data Types:**

None

**Data Breaches in New Mexico:**

- [After a month of silence, University of New Mexico assists identity theft victims](#) - The identities of more than 1000 former students and employees were stolen when a hacker gained access to an aged and now obsolete program belonging to the university's Department of Education. No fines or penalties have been reported.
- [University of New Mexico Foundation notifies community of data breach](#) - A computer server beach compromised the personal information of upwards to 23000 individuals. No penalties have been reported.
- [New Mexico AG Wants Uber to Release More Info on Data Breach](#)- In November 2017 Uber admitted to the cover-up of a year-old hacking attack responsible for stealing the personal information of approximately 57 million customers and drivers, including residents of New Mexico. Key employees were [fired](#) and the Federal Privacy Commission instigated a formal investigation. It's recently been [reported](#) that the FTC will not fine Uber for the 2016 breach. Further, it does not appear that Uber has been fined by New Mexico.
- [FRAUD ALERT: AG Balderas Warns New Mexicans of Massive Equifax Data Breach](#)- The massive Equifax data breach reported by the company in mid-2017 effected up to 57 million American across the 50 States. Numerous lawsuits have been filed. In January, 2018 the AG in New Mexico issued a fraud alert, urging New Mexicans affected by the breach to [contact the AG's office](#). To date, it appears New Mexico has not issued any penalties against Equifax.

**Pending Data Breach Legislation in New Mexico:**

None

## New York

Reference: [N.Y. Gen. Bus. Law § 899-aa](#)

### Summary:

In the state of New York, breach of the security of the system means “unauthorized acquisition” of digital data that compromises and endangers the security and privacy of personal information maintained by a business.

Proper acquisition of personal data by an employee or other authorized agent for the intended purposes is not considered a breach of security. That is provided the private information is not used or subject to unauthorized disclosure.

### Notification Requirements:

#### To Individuals:

If there is believed to be a breach of the security system, the person or entity which maintains the said information will notify the owner or licensee of the information immediately following the discovery.

The required notification may be delayed if it impedes a criminal investigation. Only after authorities determine that the notification will not compromise the investigation, will the information be released.

#### To Regulators:

The NYS Executive Budget amended section 899-aa of the General Business Law, provides that any person or entity conducting business in New York “must disclose any breaches of computerized data which includes private information” by notifying:

- The offices of the New York Attorney General,
- The New York State Division of State Police,
- The Department of the State’s Division of Consumer Protection.

If more than 5000 New York residents are affected by the breach, and need to be informed all at once, the person or business “shall also notify the consumer reporting agencies” with regard to the timing, content, and distribution of the notices and the number of affected individuals. This notice shall be made without any delay.

**Covered Information:** New York State defines “personal information,” as:

- Name
- Number
- Personal Mark, or
- Other identifier

Which can be used to identify a natural person.

“Private Information,” (is the only information that triggers a breach notification in New York State) is defined as:

- Social Security Number

- Driver's License/ or Non-Driver ID Card Number
- Account Number
- Credit Card/ Debit Card Number

#### **Penalties:**

If the attorney general believes that there has been a violation of this article, he may bring an action in the court of justice having jurisdiction to issue an injunction and restrain the continuation of such violation. In such action, "preliminary relief may be granted under article sixty-three of the civil practice law and rules." In New York State, the court may award damages and fines as the court sees fit.

#### **Special Statutes for Certain Data Types:**

##### **Data Breaches in New York:**

The Attorney General's office of New York, maintains a [list of data breaches](#) in the state.

- [A.G. Schneiderman Announces \\$575,000 Settlement With EmblemHealth After Data Breach Exposed Over 80,000 Social Security Numbers](#) – EmblemHealth suffered an incident that impacted more than 80,000 records (including more than 55,000 records of New York residents) containing Social Security numbers in a mailing error in October 2016. The state Attorney General pursued action and reached a \$575,000 settlement with the company, and EmblemHealth also agreed to implement a Corrective Action Plan and conduct a comprehensive risk assessment.

##### **Pending Data Breach Legislation in New York State:**

The following legislations relate to various aspects of the General Business Law:

A.B. 8672, A.B. 8695, A.B. 8782, S.B. 6879, S.B. 6886, S.B. 6891, S.B. 6923, S.B. 6880, A.B. 180, A.B. 7232, S.B. 1104, S.B. 6889, S.B. 6912, S.B. 7038

The following legislations relate to various aspects of Notification of a Security Breach:

A.B. 7167, S.B. 5601, A.B. 8756, A.B. 8884, S.B. 6933

The following legislations relate to Tax Laws:

A.B. 7781, S.B. 4615

The following legislation establishes the Consumer Credit Rights and Responsibilities Outreach Program:

S.B. 6914

The following legislation enacts the "personal information protection act":

S.B. 7555

## North Carolina

**Reference:** N.C. Gen. Stat. §§ [75-61](#), [75-65](#)

**Summary:** North Carolina's data breach laws are applicable to any business that conducts business within the state or owns or leases any kind of personal information of North Carolina residents.

A data breach is defined as the acquisition of personal information, whether encrypted, unencrypted, or unredacted. Good faith acquisition of information for legitimate and lawful business purposes is not classified as a breach.

### **Notification Requirements:**

#### **To Individuals:**

If a data breach is discovered, disclosure shall be made clear and conspicuous to the owner or licensee of the information without unreasonable delay. Notification may include written, electronic, or telephone. If the number of affected persons exceeds 500,000 or the cost of notifications exceeds \$250,000, a substitute notification via posting on the business website or statewide media is allowed. A delayed notification may be permissible if law enforcement determines the information may interfere with a criminal investigation.

#### **To Regulators:**

Businesses are required to inform the attorney general of any data breach with details regarding the number of affected consumers, the timing/content of the incident, along with the notification and investigation/remediation plans.

If more than 1,000 individuals are affected, the business is also required to notify all consumer reporting agencies on a nationwide basis with information about the timing/content of the incident.

**Covered Information:** Covered information includes first name or first initial and last name in combination with the following:

- Social security or employer taxpayer identification numbers
- Driver's license, State identification card, or passport numbers
- Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)
- Digital signatures
- Any numbers or information pertaining to a person's financial resources (i.e., credit card, debit card, savings account or checking account)
- Biometric data, including fingerprints

**Penalties:** The Attorney General holds responsibility for enforcement, having all powers provided in chapter 51-15 with the ability to seek any remedies provided for in that chapter. Remedies provided for under chapter 51-15 are not exclusive; other applicable penalties may apply.

### **Special Statutes for Certain Data Types:**

None

### **Data Breaches in North Carolina:**

- [North Carolina Security Breach Report 2017](#) - Hacking and phishing scams make up most of the data breaches in North Carolina in 2017. An estimated 14.2 million residents of North Carolina have been affected by data breaches since 2005.
- [The Briefcase: N.C. will receive \\$390,814 from Target data breach settlement](#) - The 2013 data breach of Target Corp. affected over 41 million customer's payment information and compromised over 60 million customer's personal contact information. North Carolina Attorney General teamed up with 46 other states to reach a grand settlement payment of \$18.5 million, with \$390,814 of that going towards North Carolina state.
- [Attorney General Stein Wins \\$120,000 For North Carolina Over Nationwide Data Breach](#) - A data breach of Nationwide Mutual Insurance Company in 2012 resulted in a loss of personal information for 1.27 million consumers. The settlement included a \$120,394 payment to the state of North Carolina and required Nationwide to take initiative towards updating security practices.

**Pending Data Breach Legislation in North Carolina:**

None



## North Dakota

**Reference:** N.D. Cent. Code §§ [51-30-01 – 07](#)

**Summary:** North Dakota data breach laws apply to any person or business that maintains, licenses or records computerized personal information.

A data breach is defined as an unauthorized acquisition of computerized personal information that is not encrypted, secured or otherwise in an unreadable or unusable condition. Good faith acquisitions of personal data are not considered a data breach as long as the information is not disclosed without further authorization.

### **Notification Requirements:**

#### **To Individuals:**

In the event of a data breach, notification must be made expediently without unreasonable delay to any resident of the state whose unencrypted personal information was acquired or was believed to have been acquired without proper authorization. Any person who maintains or licenses personal information for someone else shall immediately notify the owner or licensee of a data breach.

Disclosures to individuals may be provided either in writing or electronically. A substitute notice is acceptable if any of the following conditions are met: the cost of the disclosure exceeds \$250,000; the notification exceeds 500,000 individuals or adequate contact information is unavailable.

A substitute notice consists of the following: electronic mail notification, if electronic mail addresses are available, conspicuous posting on the person's web site, if applicable, or notification to major statewide media outlets.

A delay in individual notification may be allowed if law enforcement determines the disclosure interferes with a criminal investigation. The notice must be made after law enforcement confirms there is no further interference with an investigation.

#### **To Regulators:**

An expedited notification by mail or electronic mail to the attorney general is required if the data breach exceeds two hundred fifty state residents.

**Covered Information:** Covered personal information includes first name or first initial and last name in combination with any of the following unencrypted information:

- Social security number
- Driver's license or state issued identification numbers
- Financial account numbers with associated account password or access code
- Date of Birth
- Maiden name of individual's mother
- Medical information regarding an individuals' health history, conditions, diagnosis or treatments
- Health insurance identification or policy numbers
- Individual's employer assigned identification number with password or access code
- Digitized or other electronic signature

Personal information does not include records made publicly available through federal, state or local government entities.

**Penalties:** The attorney general may enforce penalties classified by, but not exclusive to North Dakota State [Chapter 51-15](#).

**Special Statutes for Certain Data Types:**

None.

**Data Breaches in North Dakota:**

- [More than 248,000 North Dakotans affected by Equifax data breach](#) - The September 2017 Equifax data breach exposed 143 million individuals nationwide, with more than 248,000 North Dakota residents' personal information at risk. Information included social security numbers, birth dates, addresses, and possibly more.

**Pending Data Breach Legislation in North Dakota:**

None

## Ohio

**Reference:** Ohio Rev. Code §§ [1349.19](#) – [192](#)

**Summary:** In the state of Ohio, data breach laws are applicable to any person or business that owns, licenses or records personal information in a computerized system. Information that is encrypted, redacted or otherwise altered so that identifying information is unreadable is excluded.

A data breach in Ohio is defined as an unauthorized access and acquisition of computerized personal information that compromises the security or identity of Ohio residents in which potential risk for identity fraud or other fraud may be encountered. However, good faith acquisitions of personal information or the acquisition of personal information for judicial purposes, such as subpoenas, search warrants or other court orders are not considered data breaches.

### **Notification Requirements:**

#### **To Individuals:**

Disclosure of any such data breach in which there is material risk for identity fraud or other fraud shall be made as soon as possible to residents of Ohio whose primary or recorded mailing address resides within the state. The person in charge of the disclosure may have up to forty-five days to present the notice after discovery of the breach, subject to any law enforcement involvement or investigative needs pertaining to the identifying the details of the breach.

A delay may be ensued if law enforcement determines the disclosure interferes with any criminal investigation or poses a threat to homeland or national security.

Notification may include written, telephone or electronic, if this is the primary method of contact with the Ohio resident. A substitute notice is acceptable if contact information is unavailable or if the cost of notification exceeds \$250,000 or if the notification exceeds 500,000 people. The substitute notice must include all of the following: electronic mail, conspicuous posting on the entity's website and notification to major statewide media.

If a data breach occurs at a small business with ten or fewer employees and the notification cost exceeds ten thousand dollars, then a substitute notice is also accepted. In this case, the business is required to submit a paid advertisement in the local newspaper for three weeks, post the notice on the business' website and notify major local media outlets within the geographic area of the business.

Financial institutions including trust companies, credit unions or affiliates thereof that are otherwise required by state, federal or regulatory organizations to notify their own customers and are subject to compliance examinations by their regulator are exempt from Ohio state data breach notification requirements.

In addition, any person that stores or records data on behalf of another party is required to notify the other party in the event of a data breach in an expeditious manner.

#### **To Regulators:**

If a data breach affects over one thousand Ohio residents in a single occurrence,

notification shall be made without reasonable delay to all nationwide consumer reporting agencies regarding the scope of the breach and disclosure.

**Covered Information:** Covered information includes first name or first initial and last name in combination with any of the following:

- Social security number
- Driver's license or state issued identification numbers
- Financial account numbers with associated account passwords or access codes

**Penalties:**

The attorney general has the authority to pursue civil action to persons who fail to comply with Ohio state data breach law requirements. Penalties for non-conformance may include:

- Temporary restraining order
- Preliminary or permanent injunction
- A fine of up to \$1,000 per day for the first 60 days of noncompliance
  - The fine raises to \$5,000 per day after 60 days of noncompliance
  - The fine then raises to \$10,000 per day after 90 days of noncompliance

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Ohio:**

- [Springfield Hospital Records Breach Largest in Ohio](#) - Improper disposal of 113,000 medical records in a public recycle bin at Community Mercy Health Partners exposes 94,000 patients' personal data in late 2017. Free credit monitoring was offered to those individuals affected whose sensitive was exposed.

**Pending Data Breach Legislation in Ohio:**

None

## Oklahoma

**Reference:** Ok. Stat., Tit. 24, [§§ 161–166](#)

### [Oklahoma’s Security Breach Information Act](#)

**Summary:** Oklahoma’s data breach legislation relates to the unauthorized gathering and use of unencrypted computerized personal information of anyone from the state of Oklahoma. This legislation includes the private data of any individual or entity part of a database of personal information in the state.

For a breach to occur, two factors must be met. First, the acquisition or access must compromise, or be reasonably believed to compromise the security or confidentiality of personal private information. Additionally, the unauthorized collection has caused identity theft. Or the individual or entity believes it could lead to identity theft or other fraud related crime to any resident of Oklahoma.

#### **Notification Requirements:**

If these points within the definition of a breach are satisfied, notice must be given regarding the breach. Conversely, if the definition is not met then no notice is required.

#### **To Individuals:**

Notice must be given to people from the state of Oklahoma without unreasonable delay if a breach concerning their personal information has occurred. Notice may be given by telephone, electronic notice or substitute notice via a conspicuous posting on the website or general email if certain conditions are satisfied relating to the expected cost of notification exceeding \$50,000 or the number of people affected exceeding 100,000.

The caveat to giving this notice without unnecessary delay is that priority is given to determining the scope of the breach and to restoring the reasonable integrity of the system.

Likewise, if a law enforcement agency advises the person or entity who holds the database that giving notice may impede an investigation into the breach, then the notice will be delayed until the authorities advise that investigations have been conducted and giving notice to affected persons will no longer adversely affect the investigation or jeopardize national security interests. Once this has been determined notice must be given to affected persons without unreasonable delay.

#### **To Regulators:**

None required.

**Covered Information:** Covered information includes first and last name or first initial and last name of an individual if that information has not been encrypted or redacted, that is also linked with one or more of the following:

- Social Security number
- Driver’s license or state identification card number in lieu of a license
- Financial account numbers

- Credit or debit card numbers (plus any security or access codes which if obtained would give access to financial accounts)

Covered information in the state of Oklahoma refers only to computerized data and does not apply to the same covered information in other forms.

#### **Penalties:**

Once investigations have been conducted and a data breach with injury or loss to Oklahoma residents is confirmed, it will be prosecuted by the attorney general or district attorney of Oklahoma in the same manner as a violation under the Oklahoma Consumer Protection Act.

Prosecution for these breaches is the exclusive domain of the attorney general or district attorney in Oklahoma and penalties arising from prosecution, unless otherwise specified, are limited to \$150,000 per breach of a system or a series of breaches of the same nature discovered in the course of a single investigation.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Oklahoma:**

- [Oklahoma Employment Security Commission and Office of Workforce Development](#) - There was a data breach in March 2017 relating to Oklahoma Employment Security Commission and Office of Workforce Development that affected 430,679 Oklahoma users of a Job Search site American Job link Alliance. As a result of the breach, the system was fixed and the scope of the breach was determined by a third-party vendor RSA which conducted forensic examinations and worked with the FBI on this case. The affected Oklahoma residents were notified and no penalties are recorded.

#### **Pending Data Breach Legislation in Oklahoma:**

[S.B. 614](#), if passed, will require any individual or entity which owns private data relating to citizens of Oklahoma to notify the financial institution which issued the credit or debit card of which information has been compromised. This is in addition to the existing notification to the persons whose unencrypted or unredacted data has been accessed or acquired without authority.

## Oregon

**Reference:** Or. Rev. Stat. [§§ 646A.602, 646A.604, 646A.624](#)

[Or. Rev. Stat. § 183.745](#), [Or. Rev. Stat. § 646.607](#) Oregon Unlawful Trade Practice

**Summary:** Oregon has data breach legislation that applies to any person or entity who maintains computerized personal information that is unlawfully acquired and is not encrypted or unredacted. The legislation outlines that a breach is considered if the unauthorized access has materially compromised the security, confidentiality or integrity of the personal information.

### Notification Requirements:

#### To Individuals:

Individuals whose data has been affected must be notified in the most expeditious manner following the determination that a breach has occurred. Chapter 10 of S.B. 1551 requires that notification is within 45 days of the breach being discovered. Notification is not required if it has been reasonably determined following appropriate investigations that material harm is unlikely to result to the individual following the unauthorized access of their data. This determination must be made and kept in writing for five years.

When notification is required it must be without unreasonable delay unless such notification is considered by a law enforcement agency to be likely to impede a criminal investigation. In this scenario, this request to delay notification must be made in writing by the law enforcement agency.

Affected individuals or entities must work with relevant law enforcement agencies to determine the scope of the breach, access appropriate contact information and work to restore the reasonable security, integrity and confidentiality of information.

#### To Regulators:

In addition to individual notification, in Oregon notification must also be made to consumer reporting agencies without reasonable delay for any breach involving the compromised data of more than 1000 consumers.

Additionally, notification must be made to the attorney general in the most expeditious manner if the number of consumers who must be notified is greater than 250.

**Covered Information:** Oregon has quite comprehensive considerations regarding covered information for data breaches. In all cases the breach refers to data that is accessed which is not encrypted or redacted, or which is encrypted and the key has been accessed.

In the first scenario covered information refers to a person's first name or first initial and last name in combination with any one or more of the following:

- Social security number
- Driver's license number or state ID card number issued by the Department of Transportation
- Passport number or other ID number issued by the United States

- Financial accounts, including credit card and/or debit card numbers, security codes, access codes or passwords that would permit access to any financial account of the consumer.
- Data from automatic measurements of a consumer's physical characteristics, like fingerprints, retinas, or even an iris, used to prove the consumer's identity during financial transactions.
- Health insurance policy data or any other information used to identify health insurance users.
- Any and all medical history data regarding the treatment or diagnosis of any private data.

In the second scenario covered information does not need to include the consumer's first name or initial and last name if both of the following occur:

- "Encryption, redaction, or other methods" when the data element(s) has not been rendered unusable.
- Individual data element (or several elements) would make identity theft of the consumer possible.

#### **Penalties:**

Penalties exist for individuals at a variety of levels of involvement in violation of this legislation. A person who violates or who procures, aides or abets another person in violation of this act can be penalized by not more than \$1000 for each violation which is paid to the State Treasury. This is in addition to every other extent of the law enforcement provisions.

In Oregon every breach is a separate offense with individual penalties not to exceed \$500,000.

Civil penalties for breaches are in accordance with Or. Rev. Stat. § 183.745.

Further, all penalties are cumulative and are governed by Or. Rev. Stat. § 646.607 [Unlawful Trade Practice].

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Oregon:**

Oregon has a [state database of data breaches](#) which currently runs to 203 entries. These entries include the name of the organization, the date of the breach and the date of the notification. It does not include details regarding the nature of the breach or penalties imposed.

- [Oregon to investigate LifeWise data breach](#) – The state of Oregon joins Washington and Alaska in a multi-state investigation of a breach involving LifeWise Health Plan of Oregon and its parent company Premera Blue Cross. The personal information of more than 250,000 Oregon residents was exposed in the data breach. No penalties are yet reported.

#### **Pending Data Breach Legislation in Oregon:**



[S.B. 1551, Chap. 10](#) further tightens the notification deadlines to 45 days after the breach has been detected. The legislation also prohibits credit reporting agencies from charging a fee to freeze or unfreeze credit reports when breaches have occurred.

Additionally, Amendments to Oregon’s Information Security Law, [O.R.S. 646A.622](#) have been made and will come into effect 91 days after signing. This broadens the scope of people required to notify in the event of a breach from those who “own or license personal information” to those who “otherwise possess” personal information.

Given the comprehensive nature of “covered information” under Oregon’s legislation, the new law does make an exception for HIPAA Covered Agencies who are exempt from the 45-day notification requirement and are instead bound by the HIPAA regulations of 60 days.

## Pennsylvania

**Reference:** 73 Pa. Stat. [§ 2301 et seq.](#)

Unfair Trade Practices and Consumer Protection Law.

**Summary:** Pennsylvania's data breach legislation relates to any person or entity who maintains a database of personal information of multiple persons and that information is accessed or acquired, or is reasonably believed to have been so, in an unauthorized manner. If the information accessed has been encrypted or redacted it is not a breach unless the access key has also been accessed.

A breach is defined when the above occurs and the security or confidentiality of personal data of residents of Pennsylvania are materially compromised.

### **Notification Requirements:**

#### **To Individuals:**

Notification must be made without unreasonable delay to residents of Pennsylvania when a breach concerning their data has occurred. The caveat to this is that the scope of the breach must first be determined and the security and integrity of the data system must also be reinstated.

Additionally, delay may be appropriate if a law enforcement agency has advised in writing that giving this notice to affected consumers would impede a criminal investigation or homeland security. Once such an investigation has been completed, the notification must be made without undue delay.

#### **To Regulators:**

Notice must be given without unreasonable delay to consumer reporting agencies if the number of consumers affected by the data breach exceeds 1000.

**Covered Information:** Covered information includes first and last name or first initial and last name of an individual if that information has not been encrypted or redacted, that is also linked with one or more of the following:

- Social Security number
- Driver's license or state identification card number in lieu of a license.
- Financial account numbers
- Credit or debit card numbers (plus any security or access codes which if obtained would give access to financial accounts)

Covered information in the state of Pennsylvania refers only to computerized data and does not apply to the same covered information in other forms.

### **Penalties:**

Any individuals or entities found to be acting in a manner deemed to be an unfair or deceptive act or practice will be considered to be in violation of this legislation, known as the Unfair Trade Practices and Consumer Protection Law. The Office of the Attorney General will have the exclusive right to prosecute violations of this act. No limitations are outlined to the extent of penalties for these breaches.

### Special Statutes for Certain Data Types:

None

### Data Breaches in Pennsylvania:

A number of data breaches have been reported in Pennsylvania including:

- [300,000 records breached in ransomware attack on Pennsylvania health system](#) - A Women's health group notified 300,000 Pennsylvanian residents of a data breach in their system which was detected in May 2017 but it is believed that records could have been accessed as early as January 2017. A server and workstation were discovered to have been affected by ransomware on May 16. It is believed that a range of medical information including blood type, pregnancies and lab results were accessed as well as names, Security numbers and birth dates. The health system contacted the FBI to make a report. No penalties are recorded.
- [Chipotle security breach affected 10 Philly locations](#) - Chipotle restaurants in Pennsylvania were also affected by a breach from ransomware in February 2016. It is believed that Malware designed to steal payment data affected their point-of-sale devices at most of their restaurants. Law enforcement agencies, cyber security firms and payment card institutions collaborated to address the breach. The company addressed the threat, improved security and notified relevant financial institutions. No penalty is recorded.
- [Ransomware attack hits Pennsylvania Senate Democrats](#) - Senate Democrats were affected by a breach by ransomware in March 2017. It is believed the Ransomware attack was aimed at accessing confidential information. No penalty is recorded.

### Pending Data Breach Legislation in Pennsylvania:

Pennsylvania has a number of pending legislation amendments for data breaches. They are as follows:

[H.B. 494](#) amends the act of November 29, 2006 (P.L.1463, No.163), known as the Credit Reporting Agency Act, "provides for definitions, for security freeze, for consumer reporting agency, for personal identification, for temporary access or removal of security freeze, for secure procedures and for fees, provides for construction."

[H.B. 36](#) amends the act of Dec. 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, provides for definitions.

[H.B. 1345](#) amends Title 24 (Education) of the Pennsylvania Consolidated Statutes, in preliminary provisions, provides "for student data privacy and protection, imposes duties on the Department of Education."

[H.B. 1548](#) amends the Breach of Personal Information Notification Act, provides for "definitions and for notification of breach, provides for contents and nature of notice and for storage policies."

[S.B. 308](#) amends the Breach of Personal Information Notification Act, provides "for title of act, for definitions and for notification of breach, prohibits employees of the state from using non-secured Internet connections, provides for a policy and for entities subject to the Health Insurance Portability and Accountability Act of 1996."

[H.B. 848](#) amends the act of Dec. 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, provides for notification of breach.

[H.B. 33](#) amends the act of Dec. 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act, provides for notification of breach.

[H.B. 1846](#) amends the act of Dec. 22, 2005, known as the Breach of Personal Information Notification Act, provides for “definitions and for notification of breach, provides for notification, provides for notice exemption, provides for civil relief.”

[H.B. 1847](#) amends the Credit Reporting Agency Act, provides for “definitions and for fees, provides for credit monitoring and consumer reports, prohibits the waiver of rights, and provides for civil relief.”

[H.B. 1879](#) amends the Credit Reporting Agency Act, provides for fees, provides for “reimbursements for security breaches, and provides for notices of security breaches.”

## Rhode Island

**Reference:** [R.I. Gen'l Law, tit. 11-49.3.1 et seq](#)

**Summary:** The Identity Theft Protection Act of 2015 was passed by the Rhode Island National Assembly and signed by Governor Gina Raimondo on June 26, 2015 ([the 2015 Act](#)). The act took effect in 2016, and it clarified ambiguities in the States existing identity theft laws. The Act of 2015 imposed clear and specific notification requirements should a data breach occur and broadened the various protections available to the citizens of Rhode Island.

The 2015 Act defines a data breach as the unauthorized acquisition of unencrypted, computerized data compromising the security, integrity, or confidentiality of personal information, which is in the safe keeping of a municipal or state agency or individual. This excludes most good-faith acquisitions by employees or agents.

### **Notification Requirements:**

#### **To Individuals:**

Notification must be as soon as possible after the data breach occurs, but no later than forty-five (45) days after the breach has been confirmed. Notification of the breach must be communicated to any Rhode Island resident whose personal information was accessed, or believed to have been accessed, by an unauthorized individual or entity.

Notification must include the following six elements:

- The number of affected individuals with a description of the breach and how it occurred
- The type of information that was compromised
- The date or date range of the data breach
- The date that the data breach was discovered
- An accurate description of remediation services available, including contact information
- Accurate information of a consumer's right to file or obtain a police report; the necessary steps to request a credit freeze and any fees to be paid to the consumer reporting agencies

Notification must be made in writing or electronically, Electronic notice must follow the provisions set out in [15 U.S.C. § 7001](#). A substitute notification method is permitted if the notifying party can demonstrate that using either of the methods outlined above would cost in excess of \$25,000, or the number of individuals to be notified exceeds 500,000, or there is insufficient contact information on file for a person. Acceptable substitute notification methods include the forwarding of an electronic notification to those individuals for whom the entity has a valid email address, visible publication of the notice on the reporting organization's website, or notification to major media outlets in Rhode Island.

#### **To Regulators:**

Individuals and entities that are required to issue a security breach notification to more than 500 Rhode Island residents must also notify the Attorney General and the credit reporting agencies.

If any state, federal or local law enforcement agency determines that issuing a data breach notice could hinder an active criminal investigation, the data breach notification can be delayed. Notification must be

made to the affected parties as soon as it is deemed there is no further risk to compromising the criminal investigation.

**Covered Information:** Covered information pertains to a person’s first name or initial and surname linked to one or more of the following:

- Social Security Number
- Driver’s license or a State issued identification card number
- Medical or health insurance information
- Debit or credit card account numbers (combined with matching security, access codes or passwords)
- E-mail address with corresponding security, access codes or passwords

**Penalties:** Violations are punished through actions brought forth by the state Attorney General. Civil penalties in the amount of \$100 or \$200 per violation may be imposed. There is no cap on the penalty amounts.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Rhode Island:**

- [20K notified of data breach at healthcare network Lifespan](#) - A laptop of a Lifespan employee was stolen. The laptop, containing patient information, was not password protected; nor was the information encrypted. The employee immediately notified the company and law enforcement. Lifespan issued a public statement stating that no Social Security numbers, financial information, patient diagnoses or other clinical information had been stored on the stolen device. No fines or penalties have been reported.
- [Neurology Foundation Unauthorized PHI Access Could Affect 12K](#) - The Neurology Foundation Inc., based in Rhode Island, discovered that an employee had been making unauthorized purchases on a company credit card and had transferred private patient data onto a personal hard drive. The drive was recovered, and the employee was terminated. No fines or penalties have been reported.
- [WEI Mortgage LLC \(“WEI Mortgage”\), Notification of Data Breach](#) - In September 2017 WEI Mortgage was the victim of an email phishing attack. It was determined that 2 Rhode Island residents were potentially impacted by the breach. They were instructed to contact the Rhode Island [Attorney General](#). No fines or penalties have been reported.

#### **Pending Data Breach Legislation in Rhode Island:**

[H. B. 7387/ S.B. 2497](#) is legislation pending in Rhode Island in relation to establishing procedures for notifying individuals when data breaches occur.

[H.B. 7789/ S.B. 2790](#) is legislation pending in Rhode Island which will create the “Insurance Data Security Act”, adopting the National Association of Insurance Commissioners Model Act with respect to data security. This legislation is scheduled to take effect July 1, 2018.

## South Carolina

**Reference:** [S.C. Code Ann. § 39-1-90](#)

**Summary:** Any individual or entity doing business in South Carolina who owns or licenses computerized or other data, which includes personal identifying information, is responsible for disclosing any data breach.

The South Carolina legislation defines a data breach as the unauthorized acquisition of computerized data not ceded unusable through encryption or other methods. The data intrusion places at risk the security, integrity or confidentiality of the information held by a person or entity when an illegal activity has occurred or is likely to occur. This excludes most good-faith acquisitions by employees or agents.

### **Notification Requirements:**

#### **To Individuals:**

Notification of a data breach must be communicated to consumers immediately upon discovery. The means of notification can include direct mail, telephone or electronically, if electronic communication is generally used to communicate with the customer. A substitute notification method is permitted if the notifying party can demonstrate that utilization of the methods outlined above would cost in excess of \$250,000.00 or there is insufficient contact information on file. Acceptable substitute notification methods include the forwarding of an electronic notification to those individuals for whom the entity has a valid email address, visible publication of the notice on the reporting organization's website, or notification to South Carolina's major media outlets.

In the breach notice entities should include: what happened; what personal information was compromised; what steps the entity is taking to rectify the breach; what steps consumers should take; who the consumer can contact for additional information; finally, educational resources and the availability of consumer assistance.

#### **To Regulators:**

Any individual or entity required to issue notification of a security breach to more than one thousand (1000) people at any one time shall also notify the Consumer Protection Division of the Department of Consumer Affairs along with any and all consumer reporting agencies which compile and maintain information on a national level.

If any state, federal or local law enforcement agency determines that issuing a data breach notice could hinder an active criminal investigation, the data breach notification can be delayed. Notification must be made to the affected parties as soon as it is deemed there is no further risk to compromising the criminal investigation.

**Covered Information:** Covered information includes a person's first name or initial and surname linked to one or more of the following:

- Social security number
- Driver's license number or state identification card number

- Debit or credit card account numbers (combined with matching security, access codes or passwords)
- Any other numbers or identifying information that could be utilized to access a personal financial accounts or any information issued by a government or regulatory entity which are unique to a given individual

**Penalties:** Any person or entity who deliberately fails to notify consumers within the confines of the terms stated in the legislation can be fined in the amount of \$1000 for each consumer whose information was compromised as a result of the breach.

Banks or financial institutions subject to and in compliance with the federal Gramm-Leach-Bliley Act are exempt.

South Carolina residents who are injured by a data breach violation are within their rights to:

- Launch a civil action to recover damages if the violation was deliberate.
- In the case of negligence, launch a civil action limited to damages incurred.
- Enforce compliance through a court injunction.
- If successful, complainants can further recover legal fees and court costs.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in South Carolina:**

- [South Carolina Reveals Massive Data Breach](#) - In mid-September 2012 a server at the State's Department of Revenue was accessed by an international hacker, resulting in roughly 3.6 million Social Security Number and 387,000 debit and credit cards belonging to South Carolina tax payers being stolen. Anyone who had filed an income tax since 1998 became a potential victim of identity theft. [Four Years Later, Case Still Open in DOR Data Breach](#); no fines or penalties have been reported.
- [Anthem to pay record \\$115 million to settle U.S. lawsuits over data breach](#) – A cyberattack targeting Anthem Life Insurance Company compromised the private information of South Carolina consumers who had purchased Insurance products from Anthem, Unicare Life and Health Insurance Company, and Greater Georgia Life Insurance Company. Anthem offered all customers, both current and former, access to complimentary credit protections services.
- [Data Breach Impacts 4.5 Million Patients in South Carolina and Other Southern States](#) - Community Health Services (CHS) systems reported a data breach affecting South Carolina patients treated at four South Carolina hospitals. CHS believed that the hackers did not obtain any patient records for credit card information. No fines or penalties have been reported.

#### **Pending Data Breach Legislation in South Carolina:**

[H4383](#) is a House resolution requesting the South Carolina Attorney General launch a lawsuit against credit reporting company Equifax in response to the data breach compromising the private information of at least two million South Carolina consumers.





[H4655](#) would enact the South Carolina Insurance Data Security Act.

## South Dakota

**Reference:** [SB62](#) Enacted March 21, 2018, due to take effect July 1, 2018

**Summary:** South Dakota's first data breach law is due to take effect on July 1, 2018. In the state of South Dakota any individual or business owning or licensing computerized protected information belonging to residents of South Dakota is subject to South Dakota's data breach laws.

South Dakota legislation defines a data breach as the unauthorized attainment of unencrypted computerized data, or encrypted data with the encryption key which puts at risk the confidentiality, security or integrity of covered information. This excludes good-faith acquisitions of protected information by employees or agents.

### Notification Requirements:

#### To Individuals:

Those affected must be notified no later than sixty (60) days from discovery of the data breach.

Notice may be provided in writing or electronically and must be consistent with the provisions set-out in [15 U.S.C. § 7001](#). A substitute notification method is permitted if the notifying party can demonstrate that using either of the methods outlined above would cost in excess of \$250,000 or the number of individuals to be notified exceeds 500,000, or there is insufficient contact information on file for a person. Acceptable substitute notification methods include the forwarding of an electronic notification to those individuals for whom the person or business has a valid email address, visible publication of the notice on the reporting organization's website or notification to major media outlets in South Dakota

#### To Regulators:

Any person or entity who finds it necessary to issue a security breach notification to more than two hundred and fifty (250) South Dakota residents is required to disclose the breach to the state's attorney general by regular or electronic mail. Further, all reporting agencies as defined by [15 U.S.C. § 1681a](#) in effect as of January 1, 2018 along with any and all consumer reporting agencies which compile and maintain information on a national level must receive notification.

Notification can be delayed if law enforcement determines that notification will impede a criminal investigation. Any delayed notification must take place within thirty (30) days of it being deemed that such notification will not have a negative impact on a criminal investigation.

**Covered Information:** Covered information includes a person's first name or initial and last name plus one or more of the following items:

- Social Security number
- Driver's license or state issued identification card number
- Debit, account, or credit card numbers (combined with required access or security codes)
- Health information
- Employee issued identification number (combined with security codes or passwords)
- Biometric data

In the state of South Dakota covered information refers only to private information available in an electronic format.

**Penalties:**

The South Dakota Attorney General may prosecute individuals or businesses, who fail to disclose a data breach, as a deceptive act or practice under [§ 37-24-6](#). Further, the Attorney General, on behalf of the State, may bring a civil action of not more than \$10,000 dollars per day, per violation. The Attorney General also has the authority to recover any costs and attorney fees associated with any data breach action.

Entities subject to and in compliance with the federal Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act of 1996 are exempt.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in South Dakota:**

- [Equifax breach affects 200K in SD](#) - South Dakota's Attorney General estimates two hundred thousand (200,000) South Dakota consumers were affected by the Equifax data breach. No fines or penalties have been reported.

**Pending Data Breach Legislation in South Dakota:**

South Dakota's data breach law (S.B. 62) is due to be take effect on July 1, 2018. The state will become the 49th state with data breach notification law.

## Tennessee

**Reference:** [Tenn. Code](#) §§ 47-18-2107; 8-4-119

### Summary:

Signed into Tennessee state law by the Governor of Tennessee in April, 2017 the most updated Tennessee security data breach act states that any individual or business in Tennessee is required to notify consumers only if the data breached was acquired by an unauthorized individual and was unencrypted, compromising the security, integrity and privacy of the holder of the information.

Acquisition of the information by an employee or agent for the use of the information holder is considered to be in good-faith and not a breach of data security, as long as the information is not subject to any unauthorized disclosure.

### Notification Requirements:

Tennessee's most [recent amendment](#) has extended the 45-day notification time limit by adding an extension for another 45 days if it is required legitimately by a law enforcement agency. The notification timeline has also been modified from disclosure being made in no later than 14 days to delaying it if a law enforcement agency intervenes to say that the notification will impede a criminal investigation.

If the law enforcement agency agrees not to compromise the investigation, the notification period stands at no later than 14 days to inform of the data breach.

### To Individuals:

Individuals may be informed via written notification or electronic notification (with stipulations). Substitute forms of notifications are allowed only if the holder of the information can show that the cost of providing notifications exceeds \$250,000 or the number of individuals affected by the breach goes over 500,000 individuals to be notified. It may also be allowed in the case that the information holder does not have sufficient contact information for the individual.

Substitute notifications comprise of email notices (in the case the information holder has an e-mail address of the individual), posting the notification on the information holder's primary website (if one is available) and broadcasting the notification via a statewide press release.

### To Regulators:

As per Tennessee state law, all individuals and businesses are required to inform their customers when a data breach occurs and their information is compromised. If the number of Tennessee residents exceeds 1000 in number, then the entities are also required to report the timing, distribution and content of the data breach to credit bureaus and consumer reporting agencies, without any unreasonable delay.

**Covered Information:** The first name and last name, or the first initial and last name along with one or more of the data elements below, as long as both the name and the data elements are not encrypted:

- Social security number
- Driver's license number
- Financial account number

- Credit or debit card number (in combination with passwords, security codes and/or access codes such as the PIN) that would allow access to the individual's account

Covered information does not include any information that is lawfully made public through government records, on the local, state or federal level.

#### **Penalties:**

Any individual or business directly affected by the data breach caused by the "information holder," the person or business in the state of Tennessee who owns or licenses the personal information, may file for file a private lawsuit and institute a civil action to recover actual damages due to the information holder violating the amendment, along with costs and attorney fees. They may also be subject to additional penalties and more under the Tennessee Consumer Protection Act.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Tennessee:**

- [Over 24 Tennessee Hotels Hit In Data Breach](#) — InterContinental Hotel Group reported that its hotels such as Holiday Inns, Candlewood Suites and more were hit by a data breach from Sep - Dec 2016. No penalties reported.
- [Electronic medical record system in local Tennessee hospital breached](#) — Decatur County General Hospital in Parsons, Tennessee went on record to state that its systems were compromised by an unauthorized party, potentially compromising approximately 24,000 patient records. Affected individuals were provided a year of credit monitoring online, as a precautionary measure.

#### **Pending Data Breach Legislation in Tennessee:**

[H.B. 545](#) relates to the discovery of an encryption key by an unauthorized person and how that impacts consumer protection of encrypted and unencrypted data.

[H.B. 1723](#) is education-related legislation requiring a director of schools to report a security data breach in the administration of certain assessments and tests to the Board of Education and the Commissioner of Education within 5 days of the breach being discovered.

[H.B. 2508](#) revises current legislation on notifying individuals of a security breach that contains their sensitive personal identifying data.

## Texas

**Reference:** Tex. Bus. & Com. Code §§ [521.002](#), [521.053](#)

### Summary:

In Texas, a breach of data security is defined as the unauthorized acquisition of electronic consumer data that compromises the privacy, security and integrity of the personal identifying information of an individual. The breach also covers and includes data that is encrypted, but only if the unauthorized person has been able to acquire a key to decode the data.

Acquisition of the sensitive data in good faith by an agent or an employee is excluded from being seen as a breach of data, unless it is used in a manner that is unauthorized.

### Notification Requirements:

Any person or business that owns personal information, or licenses electronic personal data in the state of Texas, is required to immediately report a data breach as soon as it occurs.

The data breach needs to be disclosed to any individual whose data has been compromised (or reasonably believed to have been compromised), as a result of being acquired by an unauthorized individual, as soon as the breach is discovered or the person or business has been notified of the breach.

In the event of a security breach, any person or business who does not own or license the electronic data, but maintains it, is also liable to immediately inform the entity that owns or licenses the data.

A delay in notification may only be allowed if a law enforcement agency determines that the notice will hinder a criminal investigation. As soon as the agency confirms the investigation will not be compromised, the notification can be made.

### To Individuals:

In both cases, whether a person or business owns or licenses the data or maintains the data, written notification can be mailed to the address of the individual whose sensitive information has been, or is believed to have been, compromised. An electronic notice, subject to stipulation, can also be given.

If the person or business is able to demonstrate that the cost of providing the notifications is exceeding an amount of \$250,000 or the people affected by the security breach are over 500,000, or they have insufficient contact information for affected individuals, then in this case the person may send email notifications if they have the email address of the individual, post the notification on their website (if they have one), and broadcast the breach on statewide media platforms.

### To Regulators:

According to Texas law, if over 10,000 people have been affected by the breach then the person or business is also required to report the data security breach to credit bureaus and consumer reporting agencies, on the timing, distribution and information contained in the notice that was sent to the affected individuals.

This notice has to be sent to the regulating entities without any unreasonable delay.

**Covered Information:** Personal information that on its own or in combination with other information discloses a person's identity, and includes an individual's:

- Name (first name and last name, or first initial and last name)
- Social security number
- Date of birth
- Maternal data such as the individual's mother's maiden name
- Government issued ID such as a driver's license
- Biometric data that may include a fingerprint, retina image or voice print
- Unique computerized ID, routing code or address
- Financial account number
- Credit card or debit card number (as well as passwords, transaction codes, or PIN number)
- Personal information relating to the physical or mental health of the individual
- Healthcare provision and payment history

**Penalties:**

A person or business failing to report a security breach in the state of Texas may be liable to civil penalties from \$2000 to \$50,000 per violation. Additionally, for every day that goes by without reasonable action for notifying affected individuals, the state can establish a civil penalty of \$100 per day for every pending notification, at up to \$250,000 per pending notification.

Based on the violation, the Attorney General also has the authority to issue a restraining order or an injunction. The Attorney General may also be entitled to recover court fees, costs, civil penalties and more from violators.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Texas:**

- [Texas hospital breach affects 277,000](#) — Decade old medical records that were slated to be destroyed, were discovered in a public dumpster. Records may have included sensitive patient data. No penalties reported.
- [Texas Health involved in data breach of 4000 patient records](#) — As a precautionary measure, Texas Health, one of the largest healthcare providers in North Texas provided 1 year of free credit monitoring to individuals whose social security numbers were breached.

**Pending Data Breach Legislation in Texas:**

None

## Utah

**Reference:** Utah Code §§ [13-44-101 et seq.](#)

### **Summary:**

In Utah, a breach of data or system security is a serious offence and is defined as an unauthorized person acquiring computerized or electronic data of an individual that compromises the security, integrity and confidentiality of the sensitive information of that given individual.

It excludes the acquiring of the personal data by an agent or employee of the entity who possesses the unencrypted data, unless the data is misused or disclosed in an unlawful manner.

Furthermore, as per the Utah Code, if the entity does not need to retain personal information they need to arrange to destroy the sensitive information by either shredding, erasing or altering the information to make it unreadable. This may not necessarily apply to certain financial institutions.

### **Notification Requirements:**

As soon as a person or business becomes aware of a security breach, they are required to conduct a prompt investigation to deem whether the sensitive data can be or will be used in an unlawful manner. If this reveals to be the case, then the entity is liable to contact each Utah resident affected by the breach.

If an entity only maintains but does not own or license the data they are required to notify the data owner or licensee.

Notification may be delayed in case a law enforcement agency intervenes to say that the breach might impede a criminal investigation. Once the agency confirms that the notice will not affect the investigation, notification has to be made without any unreasonable delay.

### **To Individuals:**

Notifications to Utah residents have to be sent by first-class mail to the most recent address on file for that individual. Notifications can be sent electronically, but conditions apply. Telephone notifications are also allowed, including the use of lawful automated dialing systems.

Utah residents may also be informed in the form of publications in the newspaper or through the entity's own notification procedures and security policies as long as the timing and methods are in compliance with the Utah Code.

If the entity is regulated by a federal or state law and maintains data security breach procedures or policies under that law, then the entity is seen in compliance if they notify affected Utah individuals under that law in the event of a data security breach.

In Utah, data protection laws also extend out of state for which there are specific rules and procedures.

### **To Regulators:**

None required.



**Covered Information:** The combination of the Utah resident's first and last name, or first initial and last name along with one or more of the data elements mentioned below, as long as the name or data element is unencrypted or unprotected to not render it as unusable or unreadable:

- Social security number
- Financial or bank account number
- Credit card or debit card number (including passwords, security codes, or PIN numbers) that would allow access to that individual's account
- Driver's license number or Utah state identification number

The above applies to both paper records and electronic records.

#### **Penalties:**

In Utah, the law is enforced by the Attorney General, meaning that there are no private lawsuits or no private right of action.

An entity found in violation of notifying affected individuals in the event of a security breach is subject to civil penalties of \$2,500 for one or more violations per individual affected and no more than \$100,000 for total violations affecting one or more individuals.

In addition to these penalties, the Attorney General may seek injunctive relief, court fees and other costs from the violating entity.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Utah:**

- [Utah Healthcare Hacking Breach Affects 780,000](#) — In April 2012, an estimated 780,000 patients were affected by a data breach out of which 280,000 had their Social Security numbers exposed. Free online credit monitoring services were given to those who had their social security numbers compromised.
- [University of Utah Hospitals and Clinics suffers massive data breach](#) — This enormous data breach in Utah in 2008 had over 1.5 million patient records compromised as a result of them being stolen from an employee's car. The costs imposed on the University totaled \$3.4 million.

#### **Pending Data Breach Legislation in Utah:**

[S.B. 207](#) provides amendments relating to the data protection of student records and requires the Utah State Board of Education to share some of this student data with the Utah Registry of Autism and Developmental Disabilities and the State Board of Regents, for adult students and those that qualify under the McKinney-Vento Homeless Education Assistance Improvements Act.

## Vermont

**Reference:** Vt. Stat. [tit. 9 §§ 2430, 2435](#)

### Summary:

In the state of Vermont, a security breach is defined as the unauthorized acquisition, or the reasonable belief of such an acquisition, of electronic data that compromises the security, integrity and confidentiality of the information. This does not include good-faith access by an employee or agent of the business as long as the information is not used for anything unrelated to the business.

Businesses, including the state of Vermont, state agencies and municipalities, private and public universities and non-profits and for-profits are all subject to the Act. However, some financial institutions are exempt from certain provisions of the Act.

### Notification Requirements:

Notification has to be made in the form of a 14-day notice to the Office of the Attorney General once the breach is discovered by the business, or the business has been notified. By statute, this preliminary notification is kept confidential.

### To Individuals:

Consumers or individuals must be notified of the breach as soon as possible and without any unreasonable delays. The maximum time period to notify individuals after a breach has been discovered, is no later than 45 days. Upon intervention from a law enforcement agency, the notification time may be delayed.

Individuals may be notified by mail and direct telephone call (no pre-recorded messages allowed) or through email, but only if mailing information or telephone number is unavailable or the primary mode of contact with the individual has been email.

Substitute notifications in the form of placing the notice on the business's public website or sending out a national Press Release are allowed only if mail or telephonic notifications would exceed \$5000 in cost, the magnitude of individuals affected exceeds 5000 individuals nationally, or enough contact information is not available to contact the individual by either phone or mail.

### To Regulators:

Major credit reporting agencies must be informed by data collectors if the notification of the security breach exceeds over 1000 consumers. The notification must be sent without unreasonable delay and should include the timing, distribution and all of the information in the notice sent to individuals.

**Covered Information:** The combination of first name and last name, or first initial and last name along with any of the below data elements:

- Social security number
- Driver's license number or non-driver identification number
- Bank/financial account number
- Credit or debit card number (along with passwords and/or access codes)

- Financial institution account passwords, access codes or PIN numbers

The front of a check which includes the individual's name, account and routing number, address and signature are also considered covered by the Act.

#### **Penalties:**

In Vermont, the Data Breach Notification Act holds the same authority as the Consumer Protection Act.

The Attorney General can potentially investigate and issue a civil subpoena, also called a Civil Investigative Demand, seeking civil penalties of up to \$10,000 for each violation committed. Everyday individuals are not informed registers as a separate violation. The Attorney General may also seek injunctive relief.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in Vermont:**

- [Equifax security breach](#) — One of the largest credit reporting agencies, Equifax, suffered a major data security breach in July, 2017. The massive breach may have affected 240,000+ Vermonters. No penalties reported.
- [Vermont Department of Labor's Job Link website data breach](#) — In March 2017, up to 180,000 accounts on a Vermont state vendor's online job portal were compromised in a data breach. Vermont was one of ten states affected by the breach involving software vendor AJLA (America's Job Alliance). Consumer data such as names, addresses, dates of birth and even social security numbers may have been compromised. No penalties reported.
- [Vermont Attorney General settles data breach enforcement action for \\$55,000](#) — A data breach at Health Net compromised the data of approximately 1.5 million people, out of which 525 were Vermont residents. In 2011, the Attorney General enforced a settlement for the sum of \$55,000 against Health Net.
- [University of Vermont data breach](#) — In May 2018, the University of Vermont reported a data breach which could possibly lead to the misuse of university usernames and passwords. No personal information was reported as compromised. As a precautionary measure, faculty and students were required to change their passwords. No penalties reported.

#### **Pending Data Breach Legislation in Vermont:**

[H.B. 147](#) is pending legislation relating to protecting consumer information and data security breaches.

[VT H.B. 765](#) is legislation involving breach of data in regards to financial technologies such as cryptocurrencies and blockchain.

[S.B. 156](#) relates to the protection of resident consumer data.

## Virginia

**Reference:** Va. Code §§ [18.2-186.6](#), [32.1-127.1:05](#)

### Summary:

A breach of data security in Virginia refers to the unauthorized access of unencrypted electronic personal information or medical information that compromises the confidentiality or security of that information, and is maintained as part of a collective database by an individual or entity (government, corporations, partnerships, LLCs, LLPs, agencies, for-profits, non-profits, associations and more), who believe the breach has or will cause theft of personal identifying data to any resident of Virginia.

Good faith acquisition of personal data by an employee or agency of an individual or an entity (as defined above), or of medical data by an employee or agency of an entity, are not seen as a breach of system security as long as the data is not subjected to any unauthorized or unlawful disclosure.

### Notification Requirements:

If an individual or entity owns or licenses personal information or an entity owns or licenses medical information and has reason to believe that the sensitive identifying data has been accessed in an unlawful manner, they must notify the Office of the Attorney General and any affected Virginia resident, without unreasonable delay, as soon as they discover or are notified about the breach.

Notification may be reasonably delayed for the individual or entity to determine the extent of the breach and try to contain it. It may also be delayed if a law enforcement agency believes it may impede a criminal investigation or national and homeland security.

In the event of a breach, any individual or entity who does not own nor license the personal/medical information but maintains it is liable to inform the owner or licensee without unreasonable delay.

Full disclosure also has to be made in the event that encrypted data is accessed in an unencrypted form or the unauthorized person has access to an encryption key and the individual or entity believes that the breach will cause theft of personally identifying data.

### To Individuals:

Notifications to affected Virginia residents by an individual or entity for breach of personal information, or by an entity for breach of medical information can be sent by mail to the latest address on file for that resident, or by telephone or electronic notice.

If sufficient contact information is not available or the costs of providing notices exceeds \$50,000 or the number of people to be notified exceed 100,000, then an email notice can be sent as long as a valid email address is available. The notification also has to be displayed prominently on the website of the individual or entity (if one exists), and it has to be broadcasted to major press outlets state-wide.

The notice must include general information about the breach, the type of personal/medical information that was acquired in an unauthorized manner, address policies in place to protect further breaches, and a telephone number that residents may call for support, if one is available. For breach of personal information, advice can be provided to residents about free credit monitoring and general information to remain vigilant.

### To Regulators:

In the case of a breach of personal information, if more than 1000 residents need to be informed at one time then the individual or entity is required to notify the Office of the Attorney General and major consumer reporting agencies on the timing, content and distribution of the notice.

For a breach of medical information, entities need to inform the Office of the Attorney General and the Commissioner of Health, without reasonable delay.

**Covered Information:** The first and last name, or first initial and last name combined with one or more unencrypted or redacted data elements below that includes a Virginia resident's:

- Social security number
- Driver's license or state identification number
- Financial account number
- Credit card or debit card details (including access data such as passwords or PIN number)
- Physical, mental or medical history
- Treatment protocols or diagnosis by a health care practitioner
- Health insurance policy number or subscriber identification number including any unique identifiers exclusive to the affected resident
- Claims or appeals history and records

### Penalties:

An individual or entity who fails to report a breach is subject to being imposed with civil penalties by the Office of the Attorney General. The penalty may not exceed \$150,000 for every breach of security in the system, or for a set of similar breaches that were all discovered at the same time during the investigation process.

### Special Statutes for Certain Data Types:

None

### Data Breaches in Virginia:

- [University of Virginia data breach exposed employee information of 1400 employees](#) — Cyber-attackers were able to gain access to the University of Virginia's human resource system in a phishing attack exposing key financial information.

### Pending Data Breach Legislation in Virginia:

None

## Washington

**Reference:** Washington Rev. Code § [19.255.010](#) et seq

**Summary:** Washington state data breach laws apply to any entity, either person or business, that conducts business within the state and also owns or licenses data that contains personal information. A notification of a data breach is not required if there is no reasonable risk of harm subjected to the consumers or if the data was encrypted and not otherwise usable and the encryption key was not compromised. Personal information does not include any information made publicly available through state, federal, or local government records.

A data breach in the state of Washington is defined as an unauthorized acquisition of data owned or maintained by a business or person that compromises the security, confidentiality or integrity of personal information. Good faith acquisitions of data are excluded from this definition as long as the personal data is not subject to further unauthorized disclosure.

### **Notification Requirements:**

#### **To Individuals:**

In the event of a data breach, notification must be made to the owner or licensee immediately or no more than 45 days following its discovery. A delay in notification may be permitted if law enforcement determines an interference with a criminal investigation.

Notifications may be provided only in the form of either written or electronic. However, if the cost of providing such notification exceeds \$250,000 dollars, or if the number of affected consumers exceeds 500,000 persons, or there is not sufficient contact information, a substitute notification is allowed. A substitute notification shall include all of the following elements: email (if available), conspicuous posting on the person or business' web page and notification to major statewide media.

A business or person that maintains their own data breach notification processes and are otherwise consistent with the timing notifications of Washington state statutes are deemed compliant with state notification requirements. In addition, Federal health insurance companies and certain financial institutions that comply with their own interagency regulations pertaining to data breach notification are also deemed compliant.

#### **To Regulators:**

If a data breach affects over five hundred Washington state residents in a single incident, notification must be made immediately to the state attorney general, or no more than 45 days after the breach. The notification to the attorney general must include the number of affected residents, or estimate if exact number is unknown, along with a single sample copy of the data breach notification.

**Covered Information:** Covered information includes first name or first initial and last name in combination with any or more of the following:

- Social security number
- Driver's license or Washington identification card number
- Financial account numbers with associated account passwords or access codes

### Penalties:

The attorney general may bring action on behalf of residents to enforce these state statutes regarding noncompliance and failure to take precautions against a breach.

### Special Statutes for Certain Data Types:

None

### Data Breaches in Washington:

- [Attorney General Reports 3 Million Washingtonians Personal Data Compromised](#) - Report finds that 3 million Washington residents were affected by data breaches between July 2016 and July 2017, which is six times the amount the previous year.
- [Attorney General Sues Uber](#) - Uber announced a data breach from a year earlier affecting 57 million US residents, including 11,000 Washington state residents. The Washington Attorney General seeks \$2,000 per violation of state data breach laws, which totals nearly \$22 million in penalties.

### Pending Data Breach Legislation in Washington:

[S.B. 6018](#) revises provisions relating to security freeze fees charged by consumer reporting agencies, repeals the requirement of payment of a fee required by a consumer reporting agency to freeze a consumer's credit report. Also requires a report about trends in data breaches including the frequency and nature of security breaches, best practices for preventing cybersecurity attacks, identity theft mitigation services available to consumers, and identity theft mitigation protocols recommended by the federal trade commission, the consumer financial protection bureau, and other relevant federal or state agencies.

[HJR 4202](#) amends the state Constitution to permit appropriations from the budget stabilization account in certain cases where there has been a breach of information technology systems.

## West Virginia

**Reference:** W.V. Code § [46A-2A-101](#) et seq.

**Summary:** Data breach laws in West Virginia apply to any person, business or entity that owns, licenses or maintains computerized data containing personal information. Notification of a data breach is required if unauthorized access is made or believed to have been made to unencrypted personal data or if the encryption key used to encrypt personal data is compromised. Personal data does not include information that is made lawfully available to the general public through federal, state or local government records.

The definition of a data breach in West Virginia is an unauthorized access and acquisition of computerized personal information that is unencrypted or redacted in which there is probable cause for identity theft or other fraud to any resident of the state. Good faith acquisition of data is not considered a data breach, as long as the information was lawfully acquired and not subject to further unauthorized disclosure.

### **Notification Requirements:**

#### **To Individuals:**

If a data breach is detected, the person or entity owning or licensing the data is required to notify affected individuals by either written mail, telephone or electronically. If the data breach is detected by someone who only maintains the data, then notification shall be made to the owner of the data for them to disclose. The notice shall be made as soon as practical without unreasonable delay, unless law enforcement determines the notification interferes with an active investigation or jeopardizes national or homeland security. After law enforcement determines it is clear to deliver the notification, it must be made without unreasonable delay.

A substitute notification is acceptable if it is determined that the cost to deliver such notification exceeds \$50,000 or if the number of affected residents exceeds 100,000 individuals, or if there is not sufficient contact information. The substitute notification must include all of the following elements: email notification (if available), conspicuous posting on the person or entity's web page and notification to major statewide media.

Any notification of a data breach must also include the following information to the affected individual:

- Description of the categories of information compromised
- Telephone number or website in which the individual may contact for further information regarding:
  - What type of personal information was maintained about the individual
  - Whether or not personal information was maintained about the individual
- Toll-free numbers and addresses for major credit reporting agencies and information about how to place a fraud alert or security freeze

An entity that maintains its own data breach notification procedures and is otherwise consistent with notification timing requirements of West Virginia state statutes or comply with federal or interagency regulations are considered in compliance.



### To Regulators:

In an instance of which there are over one thousand persons affected by a data breach, the entity must also notify all nationwide consumer reporting agencies with information concerning the timing and scope of the breach. It is not required to disclose any names or other personal identifying information to the reporting agencies.

**Covered Information:** Covered information includes first name or first initial and last name in combination with any or more of the following when the information is not encrypted nor redacted:

- Social security number
- Driver's license or state identification card number
- Financial account numbers with associated account passwords or access codes

### Penalties:

The attorney general has exclusive authority to bring action on behalf of residents. Civil action may only be pursued if it is found in court that the defendant has engaged in repeated and willful violations of this law. There is a max penalty of \$150,000 per breach of security for civil action cases.

Failure to comply with notification requirements constitutes as an unfair or deceptive act of practice and is enforceable by the Attorney General.

Any violations made by financial institutions are only enforceable by the entity's functional regulator.

### Special Statutes for Certain Data Types:

None

### Data Breaches in West Virginia:

- [West Virginia Sues Equifax](#) - The nationwide Equifax security breach affected over 148 million people, including 730,000 West Virginia residents. West Virginia Attorney General is suing Equifax for max penalties of \$150,000 per breach of security and \$5,000 for each violation of his state's Consumer Credit and Protection Act.

### Pending Data Breach Legislation in West Virginia:

None

## Wisconsin

**Reference:** Wis. Stat. § [134.98](#)

**Summary:** The state Wisconsin's data breach laws were signed into law on March 16, 2006 and became effective on March 31, 2006. The Wisconsin statute applies to entities whose primary place of business is in the state of Wisconsin and who also own, license or maintain personal information. Entities doing business in Wisconsin, whose principal place of business is not located within the State, are also legally obligated to notify any State resident when their personal information has been compromised.

Good-faith acquisition of protected information by employees or agents is excluded from this legislation.

### Notification Requirements:

#### To Individuals:

Notification must be undertaken by a corporation within forty-five days of discovering that private information has been breached. Such notification shall be provided by the entity in writing via mail, or a method previously utilized to communicate with the owner of the personal information.

#### To Regulators:

If required to notify one thousand or more Wisconsin residents of a data breach, said entity shall immediately contact all consumer reporting agencies responsible for the storage and maintenance of information on Wisconsin state residents, as contained in [15 USC 1681a\(p\)](#). Entities are not required to communicate a data breach if it is deemed to be no risk of identity theft or fraud. Notification can be delayed if requested by law enforcement, to protect an ongoing investigation or homeland security.

**Covered Information:** Covered information includes a person's first name or initial and last name plus one or more of the following items:

- Social Security number
- Driver's license or state issued identification card number
- Debit, account, or credit card numbers in combination with required access or security codes
- Biometric data
- Deoxyribonucleic acid profile (DNA); defined in [939.74 \(2d\) \(a\)](#)

**Penalties:** Any person who knowingly directly commits a data breach violation or assists another to commit a breach risks being charged and convicted of said violation.

### Special Statutes for Certain Data Types:

None

### Data Breaches in Wisconsin:

- [Confidential information of 9,500 patients at the Medical College of Wisconsin compromised](#) - A targeted attack on the Medical College of Wisconsin's email system

- resulted in the private information of 9500 patients being breached. The patient's emails included such information as names, home addresses, dates of birth, medical record numbers, health insurance information, diagnosis or medical condition and treatment information. No fines or penalties have been reported, to date.
- [Wisconsin Medicaid Data Breach Blamed On Stolen Laptop: Report](#) - Hundreds of Wisconsin residents had their covered information compromised when an encrypted laptop was stolen. Although the laptop was encrypted the computer's password was stored in the laptop bag. No fines or penalties have been reported, to date.
  - [Unity Point Health Says 16K People Could Be Affected By Data Breach](#) - As the result of an email phishing attack numerous employee emails were compromised. This breach has resulted in the personal information of upwards to 16,000 customers being put at risk. No fines or penalties have been reported, to date.

**Pending Data Breach Legislation in Wisconsin:**

[A.B. 565\(S.B.462\)](#) is legislation formed in respect to the fees associated with security freezes on consumers.

[S.B. 232](#) is legislation to determine criminal penalties when information is breached via a broadband Internet access service provider.

## Wyoming

**Reference:** Wyo. Stat. §§ [40-12-501](#) *et seq.*

### Summary:

Bills [S.F. 35](#) and [S.F. 36](#), with respect to data breach notification laws, were signed into law by the state of Wyoming on March 2, 2015, effective July 1, 2015. These two bills serve to amend data breach notifications in W.S. 40-12-502 and the definition of “Personal Identifying Information” as contained in W.S. 40-12-502.

The state of Wyoming defines a data information breach as the unauthorized acquisition of computerized data, if such acquisition compromises the privacy, integrity or security of the covered information held by an individual or entity. Further, if this breach causes, or could cause, injury or loss to a resident of Wyoming.

### Notification Requirements:

#### To Individuals:

When a data breach occurs, Wyoming residents must be notified as soon as possible after the breach has been discovered. Acceptable methods of notification are written notice or electronic mail notice. Notification can be reasonably delayed if law enforcement determines that notification could impede a criminal investigation.

Substitute notification is permissible if the cost of providing notice would exceed \$10,000 for individuals or entities based in Wyoming, \$250,000 for any out-of-state entities operating in Wyoming. Also, if the number of consumers to be notified exceed 10,000 for Wyoming based entities or 500,000 for any out-of-state entities operating in Wyoming. Lastly, if contact information is insufficient, substitute notification can be implemented. Such substitute notification shall include posting publicly via the Internet and notifying major Wyoming state news media. A toll-free information line number must also be included.

#### To Regulators:

None

**Covered Information:** Covered information includes a person’s first name or initial and last name plus one or more of the following items:

- Address
- Telephone number
- Social Security Number
- Driver’s License Number
- Federal, state, or tribal identification number
- Debit, account, or credit card numbers in combination with required access or security codes
- A birth or marriage certificate

- Medical information
- Health insurance information
- Username or email address combined with a password
- Biometric data
- Tax identification number
- Information known to be used to access data-based authentication such as security tokens or shared secrets

**Penalties:**

The Attorney General of Wyoming may instigate legal action to address any violations to the state of Wyoming's Data Breach Laws, and any other relief deemed appropriate.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Wyoming:**

- [Hackers breach Wyoming library system](#) - The library's statewide catalog was breached on October 7, 2014. The library reported that the hack was detected before any sensitive data was compromised. No fines or penalties have been reported.
- [Wyoming Game And Fish Not Affected By Data Breach](#) - After being notified of a data breach, hunters and fisherman have been told the data breach affects Idaho, Washington and Oregon; not sportsmen in Wyoming State. No fines or penalties have been reported.
- [Wyoming Medical Center reports patient record breach](#) - In February 2016, two Wyoming Medical Center employees fell victim to an email phishing scheme. Potentially, 3200 patients had their personal information compromised. No fines or penalties have been reported to date.

**Pending Data Breach Legislation in Wyoming:**

None

## District of Columbia

**Reference:** D.C. Code §§ [28-3851](#) *et seq.*

**Summary:** In the District of Columbia, data breach laws are applicable to any individual or business entity maintaining, possessing, or handling covered information, which they do not own.

The District of Columbia defines a data breach as the unauthorized attainment of computerized or other electronic data, including any equipment storing said data. Such an acquisition compromises the integrity, confidentiality or security of the covered information overseen by the individual or entity.

Good-faith acquisition of protected information by employees or agents is excluded from this legislation.

### Notification Requirements:

#### To Individuals:

Notification of a data breach must be communicated to D.C. residents as soon as reasonably possible after said breach. Acceptable modes of notification are in writing, or electronically if the customer has agreed to receiving notice in an electronic format. Such electronic notice must be consistent with the guidelines set out in [114 Stat. 641; 15 U.S.C.S. § 7001](#). Any notification must take into account the legitimate needs and concerns of law enforcement.

A substitute notification method is permitted if the notifying party can demonstrate that using either of the methods outlined above would cost in excess of \$50,000 or the number of individuals to be notified exceeds 100,000, or there is insufficient contact information on file for a person. Acceptable substitute notification methods include visible publication of the notice on the reporting organization's website, or the forwarding of an electronic notification to those individuals for whom the individual or entity has a valid email address or notifying major D.C. media outlets. Also notifying media outlets at the national level, if and when applicable.

Any individual or business entity subject to the federal Gramm-Leach-Bliley Act is exempt from this legislation.

#### To Regulators:

When, in addition to D.C. residents, in excess of 1000 consumers are required to be notified of a data breach all consumer reporting agencies must also receive notification in compliance with [§1681a \(p\)](#).

**Covered Information:** Covered information pertains to a person's first name or initial and surname, or phone number, or address linked to one or more of the following:

- Social Security Number
- Driver's license or a State issued identification card number
- Debit or credit card account numbers (combined with matching security, access codes or passwords)

#### Penalties:

In the District of Columbia data breach violations are punished through actions instigated by the state attorney general. The attorney general may recover a civil penalty not exceeding \$100.00 per violation, plus costs and lawyer's fees.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in District of Columbia:**

- [DC Whole Foods Customers Exposed In Data Breach](#) -The company reported customers may have at their payment card information exposed to an unauthorized party. No fines or penalties have been reported to date.
- [D.C. government data breach exposed nurses' Social Security numbers](#) -The personal information of hundreds of D.C. Dept of Health nurses has been mistakenly exposed to an online licensing portal. No fines or penalties have been reported to date.
- [Facebook: Half of DC potentially exposed to Cambridge Analytica hack](#) - Facebook has reported approximately 350,000 District of Columbia residents may had their Facebook information improperly shared with Cambridge Analytica. No fines or penalties have been reported to date.

**Pending Data Breach Legislation in District of Columbia:**

[B630](#) will amend Title 28 of the District of Columbia Official Code expanding the definition of covered information under the code.

## Guam

**Reference:** 9 GCA §§ [48-10](#) et seq.

**Summary:** In the U. S. territory of Guam data breach laws are applicable to any individual or entity that owns, licenses or maintains personal information. Exemptions may apply to certain types of businesses and differing requirements may be applicable to non-commercial entities.

A data breach is defined as the unauthorized access or attainment of covered information which compromises the privacy or security of said information.

The Guam statute applies only to electronic data. Further, the statute is not applicable to encrypted or redacted data.

Good-faith acquisitions of personal information by employees or agents are excluded.

### **Notification Requirements:**

#### **To Individuals:**

Guam residents must be notified of a data breach within a reasonable timeframe, taking into account any necessary measures required to ascertain the scope of the breach and to restore the system's integrity. The method of notification can include written, to a postal address contained in the individuals or entity's records, via telephone or electronically.

A substitute notification method is permitted if the notifying party can demonstrate that using any of the methods outlined above would cost in excess of \$10,000 or the number of individuals to be notified exceeds 5,000. Acceptable substitute notification methods include visible publication of the notice on the reporting organization's website, or the forwarding of an electronic notification to those individuals for whom the individual or entity has a valid email address or notifying major Guam media outlets.

Notification can be delayed if authorities determine that notification will compromise a criminal investigation, or national security interests.

#### **To Regulators:**

None

**Covered Information:** Covered information pertains to a person's first name or initial and surname, linked to one or more of the following, not encrypted or redacted:

- Social Security Number
- Driver's license or a Guam issued identification card number
- Debit or credit card account numbers (combined with matching security, access codes or passwords)



**Penalties:**

Individuals and entities may be liable for civil penalties for violations, not exceeding \$150,000 per breach or series of breaches uncovered in a single investigation. Violations may also result in either private remedies or other civil penalties.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Guam:**

- [Hyatt Hotels discovers card data breach at 41 properties](#) - In 2017, 17 (seventeen) Hyatt Hotel properties had their customers private information compromised. One of the breached properties is located in Guam. The compromised data included customer payment information. To date, no penalties or fines have been reported.

**Pending Data Breach Legislation in Guam:**

None

## Puerto Rico

**Reference:** 10 Laws of Puerto Rico §§ [4051](#) *et seq.*

**Summary:** Any individual or business entity doing business in the U.S. territory of Puerto Rico and owns, maintains, or licenses private personal information is subject to the data breach laws of Puerto Rico. Puerto Rican law defines a data breach as when access to private personal information is obtained by unauthorized individuals or business entities, resulting in the security, integrity or confidentiality of the data being compromised. In addition, any normally authorized person who accesses such information with the intent to utilize the information for illegal means is a breach.

### Notification Requirements:

#### To Individuals:

A security breach must be reported to each person affected as soon as possible after discovery, taking into consideration the measures required to restore the system's integrity.

Puerto Rican consumers affected by a data breach must be notified in writing or electronically, in compliance with the [Digital Signatures Act](#). The notice should provide a general definition of data breach in plain language and include the type of covered information compromised. Further, a toll-free number and an Internet site where consumers can seek assistance must be included in the notification.

A substitute notification method is permitted if the notifying party can demonstrate that using any of the methods outlined above would cost in excess of \$100,000 or the number of individuals to be notified exceeds 100,000. Acceptable substitute notification methods include visible publication of the notice on the reporting organization's website, or communication of the breach via media outlets, which includes how to contact the responsible entity or individual. When a breach affects a specific professional sector, the notification may be communicated via publications or outlets applicable to that particular sector.

#### To Regulators:

Responsible individuals or entities must notify the government of Puerto Rico within 10 days of any data breach. This is a non-extendable deadline.

**Covered Information:** Covered information pertains to a person's first name or initial and surname, linked to one or more of the following:

- Social Security number
- Driver's license, Puerto Rico issued identification
- Bank or any type of financial account numbers with or without passwords and access codes
- Usernames and password/access codes to both public or private information systems
- HIPAA protected medical information
- Tax information
- Employee evaluations

**Penalties:** Entities and individuals may be liable for civil penalties for violations, \$500 to a maximum of \$5000. Such fines do not negate the rights of consumers to launch court actions.

**Special Statutes for Certain Data Types:**

None

**Data Breaches in Puerto Rico:**

- [Puerto Rican Breach Affects 400,000](#) - Unauthorized access to an online Internet database resulted in a data breach affecting approximately 400,000 Puerto Ricans. The business entity responsible, a unit of Triple-S, was fined \$100,000 for the breach.
- [Another Major Triple-S Advantage Data Breach Has Occurred: 36,000 Affected](#) - As the result of a mailing error, plan members received correspondence containing the covered information of other plan members. To date, no fines or penalties have been imposed.
- [Puerto Rico's Electric Utility Hacked in Weekend Attack](#) - Although the hackers disrupted electrical service, the company reported no customer information was compromised. To date, no fines or penalties have been imposed.

**Pending Data Breach Legislation in Puerto Rico:**

[H.B. 607](#) is legislation currently pending to amends Law 234(2014) to establish the obligation of the holder of personally identifiable information from consumers, the ways to notify the consumer and the terms to do so.

## Virgin Islands

**Reference:** V.I. Code tit. [14, §§ 2208, 2209](#)

**Summary:** In the Virgin Islands, a U.S. territory, data breach laws are applicable to any individual or entity owning or licensing computerized data which includes covered information. A data breach is defined as acquiring unauthorized access to unencrypted computerized covered information. Such acquisition serves to compromise the integrity, security or privacy of the acquired information. Good-faith acquisitions of personal information by employees or agents are excluded. Publicly available information is exempt.

### **Notification Requirements:**

#### **To Individuals:**

Virgin Island residents affected by a data breach must be notified by the responsible individual or entity as quickly as possible after discovery, taking into consideration the measures required to restore the system's integrity, and the needs of local law enforcement.

Notice may be provided in writing or electronically. Electronic notice must be in accordance with [section 7001 of Title 15 of the United States Code](#).

A substitute notification method is permitted if the notifying party can demonstrate that using any of the methods outlined above would cost in excess of \$100,000 or the number of individuals to be notified exceeds 50,000. Acceptable substitute notification methods include visible publication of the notice on the reporting organization's website, email notice or communication of the breach via territory-wide media outlets.

#### **To Regulators:**

None

**Covered Information:** Covered information includes first name or initial and surname along with any of the following unencrypted data:

- Social Security Number
- Driver's License Number
- Debit, account, or credit card numbers in combination with required access or security codes

#### **Penalties:**

Customers affected by a data breach violation may initiate a civil action. All available rights and remedies are cumulative under the law.

#### **Special Statutes for Certain Data Types:**

None

#### **Data Breaches in the Virgin Islands:**

- [Virgin Islands Banks Hit by Massive Security Breach](#) - Customers of three major banks were affected by a massive data breach in the British and U.S. Virgin Islands. Many customers reported thousands of dollars stolen. To date, no fines or penalties have been reported.
- [OFFICER, NOW FIRED, ALLEGEDLY SHARED IDENTIFYING INFORMATION OF PEOPLE WHO FILED POLICE REPORTS](#) - Officer, now fired, leaked covered information of people who filed police reports in an attempt to steal identities. As a result, the Virgin Islands police department has stopped the practice of collecting social insurance numbers from individuals filing police reports. To date, no fines or penalties have been reported.

**Pending Data Breach Legislation in the Virgin Islands:**

None

# About Digital Guardian

Digital Guardian provides the industry’s only security platform that is purpose built to stop data theft. Our platform performs across the corporate network, traditional endpoints, mobile devices and into the cloud, buttressed by a big data analytics and reporting cloud service, to make it easier to see and block all threats to sensitive information.

For almost 15 years it has enabled data- rich organizations to protect their most valuable assets with a choice of on premises, SaaS or managed service deployment. Digital Guardian’s unique data awareness combined with behavioral threat detection and response, enables you to protect data without slowing the pace of your business.

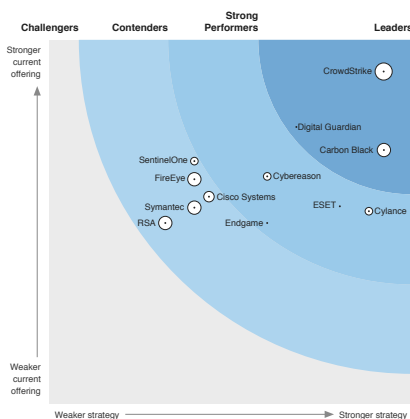
## A Recognized Leader



### “Leader” Gartner Magic Quadrant for Enterprise Data Loss Prevention

“The Digital Guardian endpoint covers DLP, advanced threat protection, and endpoint detection and response (EDR) in a single agent form factor installed on desktops, laptops and servers running Windows, Linux and Mac OS X, as well as support for VDI environments...”

Gartner, 2017 *Gartner Magic Quadrant for Enterprise Data Loss Prevention*



### “Leader” in Forrester Wave: Endpoint Detection and Response

“Digital Guardian is a newer entrant into the space and has built an extremely exciting EDR solution on top of its data loss prevention (DLP) technology. “

Forrester, *The Forrester Wave: Endpoint Detection and Response, Q3 2018*



**CORPORATE HEADQUARTERS**  
 275 Wyman St., Suite 250  
 Waltham, MA 02451 USA  
 info@digitalguardian.com  
 781-788-8180  
[www.digitalguardian.com](http://www.digitalguardian.com)

