STATE DATA SECURITY BREACH NOTIFICATION LAWS

Please note: *This chart is for informational purposes only and does not constitute legal advice or opinions regarding any specific facts relating to specific data breach incidents. You should seek the advice of experienced legal counsel when reviewing options and obligations in responding to a particular data security breach.*

Laws and regulations change quickly in the data security arena. ***This chart is current as of July 1, 2020.***

The general definition of "personal information" used in the majority of statutes is: An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state-issued identification card number, and (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account. The general definition generally applies to computerized data that includes personal information and usually excludes publicly available information that is lawfully made available to the general public from federal, state or local governments or widely distributed media. When a statute varies from this general definition, it will be pointed out and underlined in the chart.

The term "security breach" is used in this chart to capture the concept variably described in state statutes as a "security breach," "breach of the security," "breach of the security system," or "breach of the security of the system," among other descriptions.

This chart provides **general information and not legal advice** regarding any specific facts or circumstances. For more information about security breach notification laws, or other privacy and data security matters, please contact the Mintz Levin attorney with whom you work, or Cynthia Larose, CIPP/US, CIPP/E (cjlarose@mintz.com | 617.348.1732), Christopher Buontempo, CIPP/US (cjlbuontempo@mintz.com | 617.239.8322) Dianne Bourque (dbourque@mintz.com | 617.348.1614), Susan Foster, CIPP/E (sfoster@mintz.com | +44.20.7776.7330), Brian Lam, CIPP/US, FIP, CISSP (bhlam@mintz.com | 858.314.1583) or Natalie Prescott, CIPP/US (nprescott@mintz.com | 858.314.1534).

For entities doing business in Texas, be sure to review the relevant Texas law. This chart does not include information on the California Consumer Privacy Act.

Please note that rules applicable to state agencies, government bodies and other public institutions are not discussed in this chart.

- Alabama
- Alaska
- Arkansas
- Arizona
- California
- Colorado
- Connecticut
- Delaware
- District of Columbia
- 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
- Virginia
- Vermont
- Washington
- Wisconsin
- West Virginia
- Wyoming
- Puerto Rico
- Virgin Islands

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Alabama Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Alabama residents. Definition includes usernames and passwords, personal identification numbers ("PINs") or other access codes for financial accounts, medical information, and health insurance information. **Important definitions:** *"Security Breach"* means The unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach.	**Subject to statute**: A person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information of Alabama residents **Third party recipients:** Third parties maintaining personal information on behalf of a covered entity must notify covered entity about a breach and cooperate as necessary to allow covered entity to comply with statute. The covered entity must satisfy all further notification obligations under the statute.	**Written or electronic notice must be provided** to victims of a security breach as expeditiously as possible and without unreasonable delay, but **no later than forty-five (45) days following the discovery of the breach** unless law enforcement agency determines that disclosure will interfere with a criminal investigation (in which case notification delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $500,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. • **Notice not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a reasonable likelihood of harm to the consumers whose personal information was acquired**. The determination must be documented in writing and maintained for five years. **Other Obligations:** Any covered entity that must notify more than 1,000 residents at one time of a security breach is also required to notify the Attorney General and consumer reporting agencies without unreasonable delay, but **no later than forty-five (45) days following the discovery of the breach**.	**Encryption Safe Harbor:** Statute not applicable if the personal information that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. **Other exemptions**: Exemption for good faith acquisition by an employee or agent of covered entity so long as personal information is used for a legitimate purpose of employer and is not subject to further unauthorized disclosure.	**A determination of no likelihood of harm:** Does not require notification to Attorney General.	Violations by non-governmental entities constitute unlawful trade practices under the Alabama Deceptive Trade Practice Act, Chapter 19, Title 8, Code of Alabama 1975. Such entities are liable for civil penalties up to $5,000 per day for each consecutive day the entity fails to take reasonable action to comply with notice provisions, with the total civil penalty not to exceed $500,000. Damages awarded under AL Section 8-19-11 are limited to actual damages suffered by the person(s) plus attorney's fees and costs.	**Private Cause of Action:** No. Enforcement by Attorney General only.

[1] Note: Please refer to individual state statutes for a complete list of covered entities as the list of legal and commercial entities described in this chart as "subject to statute" in most cases is not exhaustive. Please also note that rules applicable to state agencies, government bodies and other public institutions are not discussed in this chart.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Alaska Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Alaska residents. Definition includes passwords, personal identification numbers ("PINs") or other access codes for financial accounts. **Important definitions:** *"Security Breach"* means an unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of the personal information maintained. *"Acquisition"* means any method of acquisition, including by photocopying, facsimile, or other paper-based method, or a device, including a computer, that can read, write, or store information that is represented in numerical form.	**Subject to statute**: Any person doing business in Alaska and any person with more than ten employees. **Third party recipients:** Third parties maintaining personal information on behalf of a covered entity must notify covered entity about a breach and cooperate as necessary to allow covered entity to comply with statute. The covered entity must satisfy all further notification obligations under the statute.	**Written or electronic notice must be provided** to victims of a security breach in the most expeditious time possible and without unreasonable delay, unless law enforcement agency determines that disclosure will interfere with a criminal investigation (in which case notification delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $150,000, affected class exceeds 300,000 persons, or covered entity has insufficient contact information. • **Notice not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a reasonable likelihood of harm to the consumers whose personal information was acquired**. The determination must be documented in writing and maintained for five years. **Other Obligations:** Any covered entity that must notify more than 1,000 residents at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies. This section does not apply to entities subject to Title V of the Gramm-Leach-Bliley Act of 1999 ("GLBA").	**Encryption Safe Harbor:** Statute not applicable if the personal information that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Safe harbor not available if the personal information is encrypted but the encryption key has been accessed or acquired. **Other exemptions**: Exemption for good faith acquisition by an employee or agent of covered entity so long as personal information is used for a legitimate purpose of employer and is not subject to further unauthorized disclosure.	**A determination of no likelihood of harm:** Requires written notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Violations by non-governmental entities constitute unfair or deceptive acts or practices under AS 45.50.471 - 45.50.561. Such entities are liable for civil penalties up to $500 per resident who was not properly notified, with the total civil penalty not to exceed $50,000. Damages awarded under AS 45.50.531 are limited to actual economic damages that do not exceed $500, and damages awarded under AS 45.50.537 are limited to actual economic damages.	**Private Cause of Action:** Yes. A person injured by a breach may bring an action against a non-governmental entity. The Department of Administration may enforce violations by governmental entities.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Arizona Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Arizona residents. Definition includes: a private key used to authenticate or sign an electronic record; individual health insurance identification number; medical information; passport number; a taxpayer identification number or PIN issued by the IRS; or unique biometric data used to access online accounts. **Important definitions:** *"Security Breach"* means an unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information maintained as part of a database of personal information regarding multiple individuals. *"Encrypt"* means to use a process to transform data into a form that renders the data unreadable or unusable without using a confidential process or key. *"Redact"* means to alter or truncate a number so that not more than the last four digits are accessible and at least two digits have been removed.	**Subject to statute:** Any legal or commercial entity that conducts business in Arizona and owns, maintains or licenses unencrypted and unredacted computerized personal information. **Third party recipients:** A person that maintains unencrypted and unredacted computerized personal information it does not own or license shall notify, as soon as practicable, the owner or licensee of the information on discovering any security system breach and cooperate with the owner or the licensee of the personal information, including sharing information relevant to the breach with the owner or licensee. The owner or licensee of the data must satisfy all further notification obligations under the statute.	**Written, e-mail or telephonic notice must be provided** to victims of a security breach within **forty-five (45) days following the determination of the breach**, unless a law enforcement agency advises the covered entity that notifications will impede a criminal investigation (on being informed by the law enforcement agency that the notifications no longer compromise the investigation, the person shall make the required notifications, as applicable, within forty-five (45) days.). • Specific requirements for the form and content of notice are described in the statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 individuals, or covered entity has insufficient contact information. • **Notice not required if the covered entity, an independent third-party forensic auditor, or law enforcement entity determines that a breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals.** **Other Obligations:** Any covered entity that must notify more than 1,000 individuals of a security breach is also required to notify the three largest nationwide consumer reporting agencies and the Attorney General.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or secured by method rendering data unreadable or unusable. **Other exemptions:** Exemption for good faith acquisition of personal information by a person's employee or agent for the purposes of the person if the personal information is not used for a purpose unrelated to the person and is not subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Arizona statute if it (i) maintains and complies with its own notification requirements as part of an information security policy that are consistent with the Arizona statute is deemed in compliance, or (ii) complies with notification requirements or procedures imposed by its primary or functional federal regulator. Entities subject to the GLBA or covered by the Health Insurance Portability and Accountability Act ("HIPAA") are exempt.	**A determination of no likelihood of harm:** Does not require notification to Attorney General.	Actual damages for a willful and knowing violation of the statute. Civil penalty not to exceed $10,000 per affected individual or the total amount of economic loss sustained by affected individuals, with a maximum civil penalty from a breach or series of related breaches of $500,000.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Arkansas Clickhere to review text of statute (*see* Ark. Code Title 4, Subtitle 7, Chapter 110, §§101 *et seq.*) Return to Index of States	**Information Covered:** Personal information of Arkansas residents. Definition includes medical information and biometric data. **Important definitions:** *"Security Breach"* means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a person or business. *"Medical Information"* means any individually identifiable information regarding medical history or medical treatment or diagnosis by a health care professional. "Biometric Data" means data generated by automatic measurements of an individual's biological characteristics.	**Subject to statute:** Any person or business that acquires, owns or licenses computerized data that includes personal information about Arkansas residents. I **Third party recipients:** Person or business maintaining (but not owning) computerized data that includes personal information must notify owner or licensee of data of any security breach immediately following discovery of security breach.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time and manner possible and without unreasonable delay, unless a law enforcement agency determines that such notification will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • **Notice not required if the covered entity determines that there is no reasonable likelihood of harm to consumers.** **Other obligations:** Data destruction or encryption mandatory when records with personal information are to be discarded. Covered entities must implement and maintain reasonable security procedures and practices to protect personal information. A person or business shall retain a copy of the written determination of a breach and supporting documentation for five (5) years from the date of determination.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. **Other exemptions:** Exemption for good faith acquisition by an employee or agent of a covered entity for a legitimate purpose so long as personal information not otherwise used or subject to further unauthorized disclosure. Entities regulated by any state or federal law that provides greater protection to personal information and similar disclosure requirements are exempt. A covered entity that maintains and complies with its own notification procedures as part of an information security policy that are consistent with the timing requirements of the Arkansas statute is deemed in compliance.	**Reasonable Likelihood of Harm:** If the breach affects the personal information of more than 1,000 individuals, the person or business then the person or business is required to make a disclosure to the Attorney General within 45 days after the person or business determines that there is a reasonable likelihood of harm. **A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Violations are punishable under the provisions of the state deceptive trade practices laws (Ark. Code 4-88-101 *et seq.*).	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
California Click here to review text statute (see Cal. Civ Code 1798.82). [California has specific statutes which could apply if medical information is compromised.] [California has specific statutes which apply to agencies. (see Cal. Civ Code 1798.29)] Return to Index of States	**Information covered:** Personal information of California residents. Definition includes medical information, health insurance information, biometric data, tax identification number, passport number, military identification number, or other unique identification number issued on a government document, and information or data collected through the use or operation of an automated license plate recognition system. Definition also captures a user name or email address in combination with a password or security question and answer that would permit access to an online account. **Important definitions:** *"Security Breach"* means an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a covered entity. Note (*eff. 1/1/2017*):: A covered entity shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption	**Subject to statute:** Any person or business that conducts business in California and owns or licenses computerized data that includes personal information. **Third party recipients:** A person or business maintaining computerized data that includes personal information that the person or business does not own must notify the owner or licensee of the information of any security breach immediately following discovery.	**Written or electronic notice must be provided** to victims of a security breach within the immediately following discovery, unless a law enforcement agency determines notification will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • Security breach notification must be written in plain English and be titled "Notice of Data Breach." It must include certain information, use specific headings, and conform to prescribed formatting. Refer to the statute for instructions and a model security breach notification form. • If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, must be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer, to any person whose information was or may have been breached if the breach exposed or may have exposed personal information involving a social security number, driver's license or California identification card numbers. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • If the personal information compromised in the data breach only includes a user name or email address in combination with a password or security question and answer (and no other personal information), then notice may be provided in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question and answer (or take other steps to protect online account).	**Encryption Safe Harbor:** A breach of encrypted data triggers a notification requirement if the encryption key or security credential is also acquired by an unauthorized person, and the owner or licensor of the affected data reasonably believes that the encryption key or security credential could be used to render the encrypted personal information readable or usable. **Other exemptions:** Exemption for good faith acquisition by an employee or agent of a covered entity so long as personal information not used or subject to further willful unauthorized disclosure. A covered entity is deemed in compliance with the California statute if it maintains and complies with its own notification procedures as part of an information security policy that are consistent with the timing requirements of the California statute. Covered entities subject to HIPAA may satisfy requirements of California statute by complying with Section 13402(f) of the federal Health Information Technology for Economic	**Attorney General must be notified if a single breach results in notification to more than 500 California residents.** Notification must be submitted online and include a sample of security breach notification to residents. Click here for required online reporting form. A **waiver** of the statute is void and unenforceable.	Civil remedies available to customers injured by a violation of the statute.	**Private Cause of Action:** Yes.

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
California, cont'd Return to Index of States	key or security credential could render that personal information readable or useable *"Medical Information"* means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. *"Health Insurance Information"* means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. *"Encrypted"* means rendered unusable, unreadable or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security. "Biometric Data" means data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate an individual.		• If the personal information compromised in the data breach only includes log in credentials for an email account furnished by the entity that has experienced the breach, then notice may be delivered to the individual online when that individual is connected to the online account from an IP address or online location from which the entity knows the resident customarily accesses the account. **Other obligations (See Cal. Civ Code 1798.81):** Businesses must implement and maintain reasonable security procedures and practices to protect personal information. Businesses responsible for data are required to take all reasonable steps to destroy a customer's records that contain personal information when the entity will no longer retain those records. A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party must require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.	and Clinical Health Act ("HITECH").			

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Colorado Click here to review text of statute (*see* Col. Rev. Stat. Title 6, Article 1, §6-1-716). Return to Index of States	**Information covered:** Personal information of Colorado residents. Definition includes (i) student, military, or passport identification number; (ii) medical information; (iii) health insurance identification number; (iv) biometric data; (v) a Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; **Important definitions:** *"Security Breach"* means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.	**Subject to statute:** A person that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. **Third party recipients:** If a covered entity uses a third-party service provider, meaning an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity, to maintain computerized data that includes personal information the covered entity in the event of a security breach that compromises such computerized data, including notifying the covered entity of any security breach in the most expedient time possible, and without unreasonable delay following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur.	**Written, electronic or telephonic notice must be provided** to victims in the most expedient time possible and without unreasonable delay, **but not later than thirty (30) days after the date of determination that a security breach occurred**, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 250,000 persons, or covered entity has insufficient contact information. • **Notice not required if** investigation determines that the **misuse of information about a resident has not occurred and is not reasonably likely to occur**. **Other obligations:** Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify in the most expedient time possible and without unreasonable delay all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal "Fair Credit Reporting Act", 15 U.S.C. sec. 1681a (p).	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted, redacted or secured by any other method rendering it unreadable or unusable. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of covered entity so long as personal information not used for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure. Entities regulated by state or federal law that maintain and comply with procedures for addressing security breaches pursuant to those laws are exempt; except that notice to the attorney general is still required. Entities subject to the provisions of the GLBA are exempt.	**A determination of no likelihood of harm:** Does not require notification to Attorney General. If the security breach is reasonably believed to have affected 500 Colorado residents or more the covered entity must provide notice of any security breach to the Colorado Attorney General in the most expedient time possible and without unreasonable delay, but not later than thirty (30) days after the date of determination that a security breach occurred. **Other exemptions, cont'd:** Any covered entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with timing requirements of statute is deemed to be in compliance with Colorado statute; except that notice to the attorney general is still required.	Attorney General may bring actions in law or equity to seek relief, including direct economic damages resulting from a violation. With either a request from the Governor to prosecute a particular case or with the approval of the District Attorney with jurisdiction to prosecute cases in the judicial district where a case could be brought, the Attorney General has the authority to prosecute any criminal violations of section 18-5.5-102.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Connecticut Click here to review text of statute *(See* Conn. Gen. Stat. §36a-701b). [For specific rules applicable to state agencies and contractors providing goods and services to a state agency – click here.] [For specific rules applicable to the insurance industry effective October 2020 – click here [*See* §230]. Return to Index of States	**Information covered:** Personal information of Connecticut residents. **Important definitions:** *"Security Breach"* means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing 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.	**Subject to statute:** Any person who conducts business in Connecticut, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information. [Connecticut has specific statutes which could apply to those engaged in the insurance business.] **Third party recipients:** If a covered entity maintains computerized data that includes personal information that the entity does not own, the entity must notify the owner or licensee of the information of any security breach immediately following discovery if the personal information was, or is reasonably believed to have been breached.	**Written, electronic or telephonic notice must be provided** to any resident of Connecticut whose personal information was breached or is reasonably believed to have been breached without unreasonable delay **but not later than ninety (90) days after the discovery of such breach** unless a shorter time is required under federal law or a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • **Notice not required if** the entity responsible for the data determines in consultation with federal, state and local law enforcement that there is **no reasonable likelihood of harm to individuals whose information has been acquired and accessed.**	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is secured by encryption or by any other method or technology that renders it unreadable or unusable. **Other exemptions:** Any covered entity that maintains and complies with its own security breach procedures that are consistent with the Connecticut timing requirements is deemed in compliance with Connecticut statute provided such covered entity notifies the Attorney General. Any covered entity that maintains its own security breach procedures pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator is deemed in compliance with the Connecticut statute provided such person notifies victims of a security breach and notifies the Attorney General.	**Attorney General must be notified not later than time notice is provided to residents.** **A determination of no likelihood of harm:** Must be made in consultation with federal, state or local law enforcement.	Failure to comply with statute constitutes an unfair trade practice.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Delaware Click here to review text of statute *(See* Del. Code Ann. tit. 6 § 12B) For specific rules applicable to the insurance industry click here (See Del. Code Ann. tit. 18 § 86) Return to Index of States	**Information covered:** Personal information of Delaware residents. Definition includes (i) passport number; (ii) medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health-care professional, or deoxyribonucleic acid profile; (iii) health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person; (iv) unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes; (v) an individual taxpayer identification number. **Important definitions:** "*Security Breach*" means the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. "*Encrypted*" means personal information that is rendered unusable, unreadable or indecipherable through a security technology or methodology generally accepted in the field of information security. "*Encryption key*" means the confidential key or process designed to render the encrypted personal information useable, readable and decipherable.	**Subject to statute:** An individual or entity that owns or licenses computerized data that includes personal information about a Delaware resident. **Third party recipients:** If a covered entity maintains computerized data that includes personal information that the covered entity does not own or license, the covered entity must notify and cooperate with the owner or licensee of the information of any security breach immediately following determination of the breach of security.	**Written, telephonic or electronic notice must be provided** to victims of a security breach without unreasonable delay but **no later than sixty (60) days following the discovery of the breach**, unless a shorter time is required by federal law, or a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $75,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. • **If a resident's Social Security number was compromised in the breach**, complimentary credit monitoring services must be offered to the resident for one year; **notice may not be given by e-mail to a resident whose related online account has been compromised**. • **Notice not required if,** after an appropriate investigation, the entity responsible for the personal information determines that **the breach of security is unlikely to result in harm to individuals whose personal information has been breached.** **Other obligations:** Covered entities must implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure or destruction of personal information collected or maintained in the regular course of business.	**Encryption Safe Harbor:** Statute not applicable if personal information subject to a security breach is encrypted, unless an unauthorized acquisition includes, or is reasonably believed to include, an encryption key that could render the personal information readable or useable. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a covered entity so long as personal information is not used for an unauthorized purpose or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Delaware statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Delaware statute.	**Delaware Attorney General must be notified if a breach involves over 500 residents.** **A determination of no likelihood of harm:** Does not require notification to Attorney General. **Other exemptions, cont'd:** A covered entity is deemed in compliance with the Delaware statute if it is regulated by state or federal law, including HIPAA and GLBA, and it complies with requirements or procedures imposed by its primary or functional state or federal regulator which are consistent with the Delaware statute.	Attorney General may bring actions in law or equity to seek appropriate relief, including direct economic damages resulting from a violation.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Florida Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Florida residents. Definition includes (i) medical history, (ii) mental or physical condition, (iii) medical treatment or diagnosis by a health care professional, (iv) health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual, and (v) a user name or e-mail address in combination with a password or security question and answer that would permit access to the account. **Important definitions:** *"Security Breach"* means unauthorized access of data in electronic form containing personal information.	**Subject to statute:** Any legal or commercial entity that acquires, maintains, stores or uses personal information. (Definition also includes government entities in some instances.) **Third party recipients:** In the event of a security breach of a system maintained by a third party agent, such third party agent must cooperate with and notify the covered entity as expeditiously as practicable but not later than ten (10) days following determination of the breach.	**Written or electronic notice must be provided** to Florida residents whose personal information was, or is reasonably believed to have been, accessed as a result of a security breach as expeditiously as practicabl but **not later than thirty (30) days following the determination of the breach.** The notification may be delayed upon the written request of law enforcement. • Specific content requirements prescribed by statute for notice to individuals. • **Substitute notice is available** by means described in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • **Notice not required if** the entity responsible for the data concludes after a reasonable investigation and consultation with federal, state and local law enforcement agencies that **the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.** **Other obligations:** Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies. Covered entities must take reasonable measures to dispose of records with personal information. A covered entity or third party contracted to maintain, store or process personal information on behalf of a covered entity must take reasonable measures to protect and secure data in electronic form containing personal information.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, secured or modified to remove elements that personally identify an individual or otherwise render the information unusable. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of covered entity so long as personal information is not used for purposes unrelated to the business or subject to further unauthorized use. Entities notifying individuals in compliance with requirements of primary or functional federal regulator are deemed in compliance with Florida requirements provided notice is timely provided to Florida Department of Legal Affairs.	**Florida Department of Legal Affairs must be notified not later than thirty (30) days after determination of breach if more than 500 Florida residents are affected.** Additional notification time may be obtained by request to the Florida Department of Legal Affairs within the 30 day period. Specific content requirements prescribed in statute for notification to Department of Legal Affairs. **A determination of no likelihood of harm:** Must be made in consultation with relevant federal, state or local law enforcement agencies. Such a determination must be documented in writing and maintained for at least 5 years. Covered entity must provide the written determination to the Florida Department of Legal Affairs within 30 days of determination.	Violations are treated as an unfair or deceptive trade practice. For failure to provide notice of the security breach within 30 days: (i) $1,000 per day for first 30 days following violation, then (ii) up to $50,000 for each subsequent 30-day period up to 180 days, then (iii) an amount not to exceed $500,000 if violation continues. Penalties apply per breach, not per affected individual. Penalties do not apply to government entities.	**Private Cause of Action:** No. Enforcement by Florida Department of Legal Affairs only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Georgia Click here to review text of statute (*see* Ga. Code Ann., Title 10, Chapter 1, §910 *et seq*.) Return to Index of States	**Information covered:** Personal information of Georgia residents. Definition includes any data elements when not in connection with a victim's first or last name if data element would be sufficient to allow someone to perform or attempt to perform identity theft. **Important definitions:** *"Security Breach"* means an unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality or integrity of personal information. *"Information Broker"* means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties.	**Subject to statute:** Any information broker that maintains computerized data that includes personal information. **Third party recipients:** Any person or business that maintains computerized data on behalf of covered entity that includes personal information that the person or business does not own must notify the covered entity who owns the information of any security breach within 24 hours following discovery of the breach.	**Written, telephonic or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. **Other obligations:** Any information broker that must notify more than 10,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of covered entity so long as personal information not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Georgia statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Georgia statute.	A state agency that has been subject to a certain single breach or aggravated computer tampering to the security of its data shall submit a comprehensive report to the attorney general and the General Assembly, specifies the content of the report, requires the report to be made available to the public.		**Private Cause of Action:** No.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Hawaii Clickhere to review text of statute. Return to Index of States	**Information covered:** Personal information of Hawaii residents. **Important definitions:** *"Security Breach"* means an incident or unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. *"Encryption"* means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. *"Redacted"* means the rendering of data so that it is unreadable or truncated so that no more than the last four digits of the identification number are accessible as part of the data.	**Subject to statute:** Any business that owns or licenses personal information of residents, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes. **Third party recipients:** Any business located in Hawaii or that conducts business in Hawaii that maintains or possesses records or data with personal information of residents that the business does not own or license must notify the owner or licensee of any security breach immediately following discovery of the breach consistent with law enforcement needs.	**Written, telephonic or electronic notice must be provided** to victims of a security breach without unreasonable delay, unless law enforcement determines that disclosure could impede a criminal investigation or jeopardize national security (in which case notification is delayed until authorized by law enforcement). • Specific requirements for the form and content of notice are described in the statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 200,000 persons, or covered entity does not have sufficient contact information. • **Notice not required if** the covered entity determines that **it is not reasonably likely that illegal use of the personal information has or will occur or it is not reasonably likely that the security breach creates a risk of harm to a person.** **Other obligations:** If more than 1,000 persons are notified at one time under the Hawaii statute, notification must also be made to applicable consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted and the confidential process or key is not also compromised.. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of covered entity so long as personal information not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure. Certain financial institutes subject to federal regulations are exempt. Any health plan or healthcare provider that is subject to HIPAA is exempt.	**Hawaii Office of Consumer Protection must be notified if a breach involves over 1000 residents.** **A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Penalties not to exceed $2,500 per violation. Violators may also be liable to injured parties for actual damages sustained as a result of the violation. Reasonable attorney fees may also be awarded to the prevailing party.	**Private Cause of Action:** No. Enforcement by the Attorney General or executive director of the office of consumer protection.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Idaho Clickhere to review text of statute. Return to Index of States	**Information covered:** Personal information of Idaho residents. **Important definitions:** *"Security Breach"* means an illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality or integrity of personal information for one or more persons. *"Primary Regulator"* of a commercial entity or individual licensed or chartered by the United States is that commercial entity's or individual's primary federal regulator. The primary regulator of a commercial entity or individual licensed by the department of finance is the department of finance. The primary regulator of a commercial entity or individual licensed by the department of insurance is the department of insurance. For all other agencies and all other commercial entities or individuals, the primary regulator is the Attorney General.	**Subject to statute:** An individual, state, or a commercial entity that conducts business in Idaho and owns or licenses computerized data that includes personal information about a resident of Idaho. **Third party recipients:** Any covered entity that maintains computerized data that includes personal information that the covered entity does not own or license must give notice to and cooperate with the owner or licensee of the information of any security breach concerning the personal information of an Idaho resident.	**Written, electronic or telephonic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay following a prompt investigation to determine if misuse of information about an Idaho resident has occurred or is reasonably likely to occur, unless a law enforcement agency determines that notice will impede a law enforcement investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $25,000, affected class exceeds 50,000 persons, or covered entity does not have sufficient contact information. • **Notice only required** if security breach materially compromises the security, confidentiality or integrity of personal information. • **Notice not required if**, after a reasonable and prompt investigation, the covered entity determines that there is **no reasonable likelihood that personal information has been or will be misused.**	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. **Other exemptions**: Exemption for good faith acquisition by an employee or agent of the covered entity so long as personal information not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Idaho statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Idaho statute. Entities regulated by state or federal law that maintain and comply with procedures for addressing security breaches pursuant to those laws are exempt.	**A determination of no likelihood of harm:** Does not require notification to Attorney General if covered entity is an individual or commercial entity.	Fine of not more than twenty-five thousand dollars ($25,000) per security breach for any covered entity that intentionally fails to give notice. Any governmental employee that intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor and, upon conviction thereof, could be punished by a fine of not more than $2,000, or by imprisonment in the county jail for a period of not more than one year, or both.	**Private Cause of Action:** No. Enforcement action brought by a covered entity's primary regulator.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Illinois Click here to review text of statute. **Important definitions, cont'd** *"Health insurance information"* means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records. Return to Index of States	**Information covered:** Personal information of Illinois residents. Definition to include (i) medical information, (ii) health insurance information, (iii) unique biometric data generated from measurements or technical analysis of human body characteristics used by the covered entity to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data, and (iv) a user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the security breach. **Important definitions:** *"Security Breach"* means an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. *"Medical information"* means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application.	**Subject to statute:** Any private university, privately held corporation, financial institution, retail operation, and any other entity that handles, collects, disseminates or otherwise deals with nonpublic personal information. **Third party recipients:** Any covered entity that maintains computerized data that includes personal information that the covered entity does not own or license must give notice to and cooperate with the owner or licensee of the personal information. Illinois may take the position that any unauthorized acquisition or use by a third party triggers the notification obligation regardless of materiality/ownership of the data.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay. Notification may be delayed if law enforcement agency determines notification will interfere with a criminal investigation and such agency provides the covered entity with a written request. • Notice to affected residents is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity does not have sufficient contact information. • If user name(s) or email address in combination with password(s) or security question(s) and answer(s) constitute the extent of the security breach, notice may be provided in electronic form pursuant to the Illinois statute. **Other obligations:** A covered entity must dispose of material containing personal information in a manner that renders the personal information unreadable, unusable and undecipherable. A covered entity must implement and maintain reasonable security measures to protect personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure. Any contracts that the covered entity has with third party recipients must require reasonable security measures for the protection of personal information.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is fully encrypted or redacted. Safe harbor will not be applicable if the keys to unencrypt or unredact or otherwise read the personal information have also been acquired without authorization. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of covered entity for a legitimate purpose of the covered entity so long as personal information is not used for a purpose unrelated to covered entity's business and is not subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Illinois statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Illinois statute.	**A determination of no likelihood of harm:** Notice in the "most expedient time possible" (but in no event later than notice to consumers). must be given to the Attorney General when 500 or more Illinois residents are affected by a single breach of a security system. Statute contains specific content required in notice A **waiver** of the statute is void and unenforceable. **Other exemptions** The data security provisions of the Illinois statute will not apply to a covered entity subject to a state or federal law requiring greater protection for records containing personal information or to covered entities that are subject to the GLBA. Covered entities subject to HIPAA are exempt from the entirety of the Illinois statute provided that any covered entity or business associate required to notify the Secretary of Health and Human Services also provides notification to the Illinois Attorney General within five (5) business days of notifying the Secretary.	A violation of the statute constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.	**Private Cause of Action:** No.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Indiana Click here to review text of statute *(see* Ind. Code, Title 24, §§ 24-4.9 *et seq.*) [For specific rules applicable to state agencies – *see* Ind. Code Title 4, §§ 4-1-11 *et seq.*] Return to Index of States	**Information covered:** Personal information of Indiana residents. Definition includes an unencrypted or unredacted Social Security Number standing alone. **Important definitions:** *"Security Breach"* means an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. Definition includes the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm or a similar media, even if the transferred data are no longer in a computerized format. Unauthorized acquisition of an encrypted portable electronic device on which personal information is stored is not a security breach if the encryption key has not been compromised. *"Encrypted"* means data that have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or data which are secured by another method that renders data unreadable or unusable. *"Redacted"* means data have been altered or truncated so that no more than last four digits are accessible (or last five digits for social security numbers).	**Subject to statute:** Any person or legal entity using computerized personal information of an Indiana resident for commercial purposes. **Third party recipients:** Any covered entity that maintains computerized data that includes personal information but does not own or license the data must notify the owner or licensee of a security breach.	**Written, electronic, telephonic or facsimile notice must be provided** to victims of a security breach without unreasonable delay, unless a law enforcement agency or the Attorney General determines that notice will impede a civil criminal investigation or jeopardize national security. Notification must occur as soon as possible after delay is no longer necessary or authorized by Attorney General or law enforcement agency. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity does not have sufficient contact information. • **Notice only required if** the covered entity knows, should know, or should have known that the unauthorized acquisition constituting **the breach has resulted in or could result in identity deception, identity theft or fraud affecting the Indiana resident.** **Other obligations:** Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies. Covered entity must implement and maintain reasonable procedures to protect and safeguard personal information of Indiana residents. Covered entity must dispose of records or documents containing unencrypted or unredacted personal information by shredding, incinerating, mutilating, erasing or otherwise rendering personal information illegible or unusable.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Safe harbor not available if encryption key has been compromised. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of covered entity so long as personal information not used or subject to further unauthorized disclosure. Covered entity is exempt if it maintains and complies with its own data security procedures as part of an information privacy and security policy or compliance plan under USA Patriot Act, Executive Order 13224, Driver's Privacy Protection Act (18 U.S.C. 2721), Fair Credit Reporting Act (15 U.S.C. 1581), Financial Modernization Act of 1999 (15 U.S.C. 6801), or HIPAA, provided the procedures are reasonable.	**Attorney General must be notified of any security breach using a designated form.** Click here for form. **A determination of no likelihood of harm:** Does not require notification to Attorney General.	Violations are actionable deceptive acts. For violations of the notification rules: The Attorney General may bring an action to enjoin future violations of the statute, a civil penalty of not more than $150,000 per deceptive act, and the Attorney General's reasonable costs. For violations of the record retention rules: The Attorney General may bring an action to enjoin future violations of the statute, a civil penalty of not more than $5,000 per deceptive act, and the Attorney General's reasonable costs.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Iowa Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Iowa residents. Definition includes (i) unique electronic identifier or routing code in combination with any required security code, access code or password permitting access to an individual's account, and (ii) unique biometric data, such as a fingerprint, retina or iris image, or other unique physical or digital representation of biometric data. **Important definitions:** *"Security Breach"* means unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the personal information. Definition includes information maintained in any medium, including on paper, that was transferred by the person to that medium from computerized form. *"Encryption"* means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. *"Redacted"* means altered or truncated so that no more than five digits of a social security number or the last four digits of other sensitive numbers are accessible.	**Subject to statute:** Any person or legal business entity that owns or licenses computerized data that includes a consumer's personal information that is used in the course of business, vocation, occupation or volunteer activities. **Third party recipients:** Any covered entity who maintains or otherwise possesses personal information on behalf of another covered entity must notify the owner or licensor of the information of any security breach of a consumer's personal information immediately following discovery of security breach.	**Written or electronic notice must be given** to any consumer whose personal information was included in the information that was breached in the most expeditious manner possible and without unreasonable delay, unless a law enforcement agency determines that notification will impede a criminal investigation and the agency has made a written request that the notification be delayed (in which case notification is delayed until authorized by law enforcement). • Specific requirements for the content of the notice are detailed in the statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 300,000 persons, or covered entity does not have sufficient contact information. • **Notice not required if** the covered entity determines, after appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, that **no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach**. Such a determination must be documented in writing and the documentation must be maintained for five years.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was breached was encrypted, redacted or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable and the keys to unencrypt, unredact or otherwise read the data elements have not been compromised. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee of a covered entity for purposes of the covered entity so long as personal information is not used in violation of applicable law or in a manner that harms or poses a threat to the affected resident. Iowa statute does not apply to a covered entity who complies with notification requirements imposed by its primary or functional federal regulator, or with other state or federal laws, that provide greater protection to personal information and at least as thorough disclosure requirements as required by the Iowa statute. A covered entity who complies with the GLBA is exempt.	**Director of Consumer Protection Division of Attorney General must be notified within five (5) business days if giving notice of a security breach to more than 500 residents.** **A determination of no likelihood of harm:** Does not require notification to Attorney General for individuals or commercial entities.	Violation is an unlawful practice. Attorney General may seek and obtain an order that a violator pay damages to the Attorney General on behalf of a person injured by the violation.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Kansas Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Kansas residents. Definition includes financial account number or credit card/debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account. **Important definitions:** *"Security Breach"* means unauthorized access to and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information and that causes, or the covered entity reasonably believes has caused or will cause, identity theft to any consumer. *"Encrypted"* means transformation of data through the use of algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable. *"Redacted"* means the alteration or truncation of data so that no more than five digits of a social security number, or the last four digits of a driver's license number, state identification number or account number are accessible as part of the personal information.	**Subject to statute:** A person or legal entity that conducts business in Kansas that owns or licenses computerized data that includes personal information. **Third party recipients:** An individual or commercial entity that maintains or otherwise possesses personal information that the individual or commercial entity does not own must notify the owner or licensee of the information of any security breach following discovery of unauthorized access and acquisition of personal information.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 5,000 persons, or covered entity does not have sufficient contact information. • **Notification is not required if,** after a reasonable and prompt investigation, the covered entity determines **it is not reasonably likely that misuse of the personal information has or will occur.** **Other obligations:** Any person that must notify more than 1,000 persons at one time of a security breach is also required promptly to notify consumer reporting agencies. A covered entity must take reasonable steps to destroy or arrange for destruction of customer's records within its custody or control containing personal information by shredding, erasing or otherwise modifying personal information so it is no longer readable or decipherable.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. **Other exemptions**: Kansas statute does not apply to an individual or commercial entity who complies with notification requirements imposed by its primary or functional federal regulator. Kansas statute does not apply to an individual or commercial entity that maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Kansas statute.	**A determination of no likelihood of harm:** Does not require notification to Attorney General.	Attorney General empowered to bring actions in law or equity to address violations. The Kanas insurance commissioner has sole authority over insurance companies who violate the Kansas statute.	**Private Cause of Action:** No.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Kentucky Click here to review text of the statute. [For specific rules applicable to government agencies – click here.] Return to Index of States	**Information covered:** Personal information of Kentucky residents. [For NTPs (see below), definition also includes first name or first initial and last name, or personal mark, or unique biometric or genetic print or image, in combination with typical data elements or one or more of the following: (i) taxpayer ID number that incorporates a SSN, (ii) state ID card number or any other individual ID number issued by any agency, (iii) passport number or other ID number issued by the USG, (iv) or individually identifiable health information as defined in HIPAA (except education records covered by FERPA).] **Important definitions:** *"Security Breach"* means unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by the covered entity as part of a database regarding multiple individuals that actually causes, or leads the covered entity to reasonably believe has caused or will cause, identify theft or fraud against a Kentucky resident. *"Nonaffiliated Third Party (NTP)"* means any person that has a contract or agreement with (and receives personal information from) a government agency, subdivision, instrumentality or unit, including such institutions as a public school or public institute.	**Subject to statute:** Any person or business entity that conducts business in Kentucky. Also covered are NTP's per KRS §61.931. **Third party recipients:** A covered entity that maintains or otherwise possesses personal information that the individual or commercial entity does not own must notify the owner or licensee of the information of any security breach as soon as reasonably practicable following discovery of security breach.	**Written or electronic notice must be provided** to victims of a security breach in the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity does not have sufficient contact information. • **Notice only required** by a security breach that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud. **Other obligations:** A covered entity that must notify more than 1,000 consumers at one time of a security breach is also required to promptly notify all consumer reporting agencies of the security breach. A business disposing of customer records must take reasonable steps to destroy the records with personal information by shredding, erasing or otherwise modifying the personal information to make it unreadable or indecipherable.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted. **Other exemptions**: Exemption for good faith acquisition by an employee or agent of the covered entity for the purposes of the covered entity, so long as personal information is not used or subject to further unauthorized disclosure. Kentucky statute does not apply to an individual or commercial entity that maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Kentucky statute. Entities subject to the provisions of the GLBA are exempt. Entities subject to the provisions of HIPAA are exempt.	[An NTP must notify its contracting agency or institution within 72 hours of determining that a breach occurred. The contracting agency or institution is responsible for notifying affected individuals.] **A determination of no likelihood of harm:** Does not require notification to Attorney General.	Attorney General may seek equitable and/or legal remedies.	**Private Cause of Action:** No.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Louisiana Click here to review text of statute. Click here to review additional rules (*see* La. Admin. Code, Title 16, § 701) Return to Index of States	**Information covered:** Personal information of Louisiana residents. Definition includes (i) passport number, (ii) biometric data. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account. **Important definitions:** *"Security Breach"* means the compromise of the security, confidentiality or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to personal information maintained by an agency or person.	**Subject to statute:** Any person or legal entity that owns or licenses computerized data that includes personal information. **Third party recipients:** Any covered entity that maintains computerized data that includes personal information that the covered entity does not own must notify the owner or licensee of the information following discovery of a security breach.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay **but not later than sixty (60) days from the discovery of the breach**, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement and the person or agency shall provide the attorney general the reasons for the delay in writing within the sixty (60) day notification period). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 100,000 persons, or covered entity does not have sufficient contact information. • **Notice not required if** the covered entity responsible for the data concludes after a reasonable investigation that there is **no reasonable likelihood of harm to residents of Louisiana.** The person or business shall retain a copy of the written determination and supporting documentation for five years from the date of discovery of the breach. **Other Obligations:** A covered entity must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure and must take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of the covered entity for the purposes of the covered entity, so long as personal information is not used or subject to further unauthorized disclosure. Covered entity deemed in compliance with the Louisiana statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Louisiana statute. Financial institutions subject to and in compliance with federal interagency guidelines are exempt.	**Consumer Protection Section of Attorney General must be notified of a security breach within ten (10) days of distribution of notice to affected Louisiana citizens.** Notice must include details of breach and names of all Louisiana citizens affected by the breach. **A determination of no likelihood of harm:** Does not require notification to Attorney General.	Civil action may be instituted to recover actual damages. Failure to provide timely notice punishable by a fine not to exceed $5,000 per violation. Notice to state Attorney General will be "timely" if received within ten (10) days of distribution of notice to Louisiana citizens. Each day notice is not received by Attorney General is deemed a separate violation.	**Private Cause of Action:** Yes.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Maine Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Maine residents. Data elements alone are considered personal information if the data would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. Definition does not include 3rd party claims databases maintained by property and casualty insurers. **Important definitions:** *"Security Breach"* means unauthorized acquisition, release or use of an individual's computerized data that contains personal information that compromises the security, confidentiality or integrity of the personal information. *"Encryption"* means the disguising of data using generally accepted practices. *"Information Broker"* means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties.	**Subject to statute:** Any information broker, individual, legal entity and private colleges and universities that maintain computerized data that includes personal information. **Third party recipients:** Any third party entity that maintains, on behalf of a covered entity, computerized data that includes personal information that the third party does not own must notify the owner following discovery of a security breach.	**Written or electronic notice must be provided** to victims of a security breach as expediently as possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification may be delayed for no longer than seven (7) business days after a law enforcement agency authorizes the notification). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $5,000, affected class exceeds 1,000 persons, or covered entity does not have sufficient contact information. • **Notice not required if,** after a reasonable and prompt investigation, the covered entity determines that there is **no reasonable likelihood that personal information has been or will be misused.** **Other obligations:** Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. **Other exemptions**: Exemption for good faith acquisition, release or use of personal information by employee or agent acting on behalf of covered entity so long as personal information is not used for or subject to further unauthorized disclosure. Covered entity deemed in compliance with the Maine statute if it complies with other federal or state security breach notification requirements at least as protective as Maine statute.	**Attorney General or Department of Professional and Financial Regulation must be notified of a security breach.** Information brokers must notify the Department of Professional and Financial Regulation and all other covered entities must notify the Attorney General. **A determination of no likelihood of harm:** Does not require notification to Attorney General.	Fines of not more than $500 per violation, up to a maximum of $2500 per each day covered entity is in violation of statute. Equitable relief and enjoinment from future violations are also available.	**Private Cause of Action:** No. The statute is enforced by the Department of Professional and Financial Regulation as to licensed data brokers and by the Attorney General as to all others.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Maryland Click here to review text of statute (*see* Md. Code Com. Law, Title 14, §§ 14-3501 *et seq.*) [For specific rules applicable to state and government agencies – *see* also Md. State Govt. Code, Title 10, §§ 10-1301 *et seq.*] Return to Index of States	**Information covered:** Personal information of Maryland residents Definition includes: • Individual Taxpayer Identification Number. • Passport Number and other ID numbers issued by federal govt • State ID card numbers • Health information (any information created by an entity covered by HIPAA regarding an individual's medical history, condition, treatment or diagnosis • A health insurance policy, certificate, number or health insurance subscribe number in combination with a unique ID that permits access to the information • Biometric data • User name or email address in combination with a password or security Q&A **Important definitions:** *"Security Breach"* means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. *"Encrypted"* means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key.	**Subject to statute:** Any business that owns or licenses personal information of an individual residing in Maryland. **Third party recipients:** A business that maintains computerized data that includes personal information that the business does not own or license must notify the owner or licensee of the information of any security breach if it is likely that the breach has resulted or will result in misuse of personal information of a Maryland resident.	**Written, electronic or telephonic notice must be provided** to victims of a security breach as soon as reasonably practicable after the business discovers or is notified of the breach of the security of a system, unless a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement agency). • Specific requirements for the content of the notice are detailed in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 175,000 persons, or covered entity does not have sufficient contact information. • **Notification not required if,** after investigation, the business determines that **misuse of the personal information has not occurred or is not reasonably likely to occur.** Records of such determination must be maintained for three years. **Other obligations:** If the business that incurs the security breach is not the owner or licensee of personal information, that business may not charge the relevant owner or licensee for information necessary to carry out the owner or licensee's notification obligations under the breach law. Owners and licensees of computerized data are prohibited from using information relative to a breach for purposes other than: 1) providing notification of the breach; 2) protecting or securing personal information; or 3) providing notification to national information security organizations to alert and avert new or expanded breaches. Any business that must notify more than 1,000 consumers at one time of a security breach is also required to notify consumer reporting	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of a business for the purpose of the business so long as personal information is not used or subject to further unauthorized disclosure. A business that is subject to and in compliance with § 501(b) of the GLBA, § 216 of the federal Fair and Accurate Transactions Act, 15 U.S.C. § 1681w, will be deemed to be in compliance with the Maryland statute. Any business that complies with the notification procedures imposed by its primary or functional federal or state regulator is deemed in compliance with the Maryland statute.	**Attorney General must be notified of a security breach prior to giving required notification to affected individuals.** **A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Violations constitute an unfair or deceptive trade practice under Title 13 of the Maryland Code.	**Private Cause of Action:** Yes Appropriate penalties and damages may be assessed in an enforcement action brought by the Attorney General. Consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act.

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Maryland, cont'd Return to Index of States			agencies of the security breach without unreasonable delay. Businesses must implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of its business. Businesses must take reasonable steps to protect personal information when destroying customer records.				

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Massachusetts Click here to review text of statute. ***Click here for text of amendment effective 4/11/19*** Return to Index of States	**Information covered:** Personal information of Massachusetts residents. Definition includes financial account number or credit/debit card number with or without any required security or access code or password that would permit access to a resident's financial account. **Important definitions:** *"Security Breach"* means unauthorized acquisition or unauthorized use of unencrypted data, or of encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a Massachusetts resident. *"Data"* means any material upon which written, drawn, spoken, visual or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics. "*Encrypted*" means the transformation of data through the use of a 126-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key.	**Subject to statute:** A person that owns or licenses data that includes personal information about a Massachusetts resident. **Third party recipients:** A person that maintains or stores but does not own or license data that includes personal information about a Massachusetts resident must provide notice of a security breach to the owner or licensor of the data as soon as practicable and without unreasonable delay and also cooperate thereafter.	**Written or electronic notice must be provided** to victims of a security breach as soon as practicable and without unreasonable delay after the covered entity discovers or is notified of a security breach, unless a law enforcement agency determines that the notification will impede a criminal investigation and has notified the Attorney General in writing of such determination (in which case notification is delayed until authorized by law enforcement agency). Entities cannot delay notifications required "on the grounds that the total number of residents affected is not yet ascertained." Notice content is specifically set forth in the statute. **Notice to AG/OCABR:** The notice shall include, but not be limited to: • the nature of the breach of security or unauthorized acquisition or use; • the number of residents of MA affected by such incident at the time of notification; • the name and address of the person or agency that experienced the breach of security; • the name and title of the person or agency reporting the breach of security, and their relationship to the person or agency that experienced the breach of security; • the type of person or agency reporting the breach of security; • the person responsible for the breach of security, if known; • the type of personal information compromised, including, but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data;	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted and the process or key that is capable of unlocking the data has not been compromised. **Other exemptions**: Covered entity is deemed in compliance with the Massachusetts statute if it maintains and complies with procedures for responding to a breach of security pursuant to federal laws and regulations provided the covered entity notifies the Attorney General and the Director of the Office of Consumer Affairs and Business Regulation of the security breach as soon as practicable and without unreasonable delay following discovery of the security breach. Notice must describe the steps to be taken.	**Attorney General and Office of Consumer Affairs and Business Regulation ("OCABR") must be *separately* notified of a security breach as soon as practicable after becoming aware of security breach.** Notice to the OCABR must be submitted through an online portal – click here. Notice to AG may either be by letter or through an online portal – click here. Notice to regulators may be required even in cases where security breach involves encrypted data. Covered entity must be able to determine that the key or confidential process has **not** been compromised. The covered entity must also provide notice to any consumer reporting agencies and state agencies identified by the OCABR. **A determination of no likelihood of harm:** Does not require notification to Attorney General.	Attorney General may bring an action under Chapter 93A, the Commonwealth's consumer protection statute. Chapter 93A permits the imposition of significant fines, injunctive relief and attorneys' fees A civil penalty of $5,000 may be awarded for each violation (*see* 93A § 4). Businesses can be subject to a fine of up to $50,000 for each instance of improper disposal of data (*see* 93I §2).	**Private Cause of Action:** Potentially. If Attorney General finds violation of consumer protection laws for unfair or deceptive acts or practices, Massachusetts consumers may seek damages under Chapter 93A, which, in some cases, may be trebled. Note: The OCABR has launched a web-based public archive of data breaches affecting Massachusetts residents: click here. Upon receipt of notice, the director of the OCABR shall report the incident publicly on its website and make available electronic copies of the sample notice sent to consumers on its website.

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Massachusetts, cont'd Return to Index of States			• whether the person or agency maintains a written information security program; and • any steps the person or agency has taken or plans to take relating to the incident, including updating the written information security program. • certification that credit monitoring services comply with the law's requirements for providing credit monitoring to individuals if social security numbers are affected. **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity does not have sufficient contact information. **Notice only required** after a security breach that causes substantial risk of identity theft or fraud or after a covered entity has reason to know that the personal information of a Massachusetts resident was acquired by an unauthorized person or used for an unauthorized purpose. **Other obligations:** Paper records containing personal information must be redacted, burned, pulverized or shredded. Electronic data containing personal information must be destroyed or erased. **Credit monitoring**: If SSNs are compromised, the breached entity must contract with a third party to provide affected individuals with no less than 18 months of credit monitoring services (42 months if the affected entity is a consumer reporting agency)				

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Massachusetts, cont'd 201 CMR 17.00 establishes minimum standards for safeguarding personal information in both paper and electronic form. Return to Index of States	**Information covered:** Personal information of Massachusetts residents. Definition includes financial account number or credit/debit card number with or without any required security or access code or password that would permit access to a resident's financial account.	**Subject to statute:** Every person or legal entity that owns, licenses, stores or maintains personal information about a Massachusetts resident. **Third party recipients:** Covers third-party service providers with access to personal information.	**The regulations require the development, implementation and maintenance of a comprehensive information security program** consistent with industry standards and state or federal regulations applicable to the covered entity with respect to owning or licensing personal information. *See* 201 CMR 17.00 for a detailed description of content requirements and technology requirements for the comprehensive information security program. The sufficiency of a comprehensive information security program will be evaluated by taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information. **Other obligations:** Requires entities to collect and store the minimum amount of personal information necessary to accomplish the legitimate purpose for which it was collected, and requires entities to restrict access to the personal information to the smallest possible number of users.	**Encryption Requirements:** The regulations require the encryption of all transmitted records and files containing personal information, including those in wireless environments, which will travel across public networks. For files containing personal information on a system that is connected to the Internet, there must be firewall protection with up-to-date patches, including operating system security patches. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the lawful purposes of the covered entity so long as personal information is not used in an unauthorized manner or subject to further unauthorized disclosure.		Please see above for a summary of applicable penalty provisions of Mass. Gen. Laws. c. 93A, c. 93H and c. 93I.	**Please see above.** Consumers may seek damages under Mass. Gen. Laws. c. 93A.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Michigan Click here and here to review text of statute. Return to Index of States	**Information covered:** Personal information of Michigan residents **Important definitions:** *"Security Breach"* means unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a covered entity as part of a database of personal information regarding multiple individuals. *"Encrypted"* means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable. *"Redact"* means to alter or truncate data so that no more than four sequential digits of a driver license number, state personal identification card number, or account number, or no more than five sequential digits of a social security number, are accessible as part of personal information.	**Subject to statute:** Any person or legal entity that owns or licenses personal information that is included in a database. **Third party recipients:** A covered entity that maintains a database that includes data that the person does not own or license must notify the owner or licensor of the information of a security breach unless the covered entity determines that breach has not or is not likely to cause substantial loss or injury to, or result in, identity theft with respect to, one or more Michigan residents	**Written, electronic or telephonic notice must be provided** to victims of a security breach without unreasonable delay. Notification may be delayed if law enforcement agency determines that notification will impede a criminal or civil investigation or jeopardize homeland or national security. Notification must occur without unreasonable delay following authorization from the law enforcement agency. • Notice to affected residents is required to contain specific content described in the statute. • Covered entities may deliver notice pursuant to an agreement with another covered entity, if the agreement does not conflict with the MI statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000 or affected class exceeds 500,000 persons. • **Notification is not required if** the covered entity determines that breach has not or is **not likely to cause substantial loss or injury to, or result in, identity theft with respect to, one or more Michigan residents**. In making this determination, a covered entity must act with the care an ordinarily prudent person in like position would exercise under similar circumstances. **Other obligations:** Any covered entity that must notify more than 1,000 residents at one time of a security breach is also required to notify consumer reporting agencies of the security breach without unreasonable delay (unless subject to GLBA).	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted and the encryption key was not compromised. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity related to their activities for the covered entity so long as employee or agent does not misuse personal information or disclose any personal information to an unauthorized person. Financial institutions that are subject to and comply with notification procedures from an appropriate regulator are exempt from Michigan statute. A covered entity that is subject to and complies with HIPAA is exempt from Michigan statute.	**A determination of no likelihood of harm:** Does not require notification to Attorney General for individuals or commercial entities. A **waiver** of the statute is void and unenforceable.	Civil penalty for failure to provide notice of not more than $250 for each failure to provide notice, capped at $750,000 per security breach. Penalties do not affect availability of civil remedies under state or federal law. Criminal penalties for notice of a security breach that has not occurred, where such notice is given with the intent to defraud. Misdemeanor – 93 days imprisonment or fine of $250 (or both) for each violation (penalties escalate with more violations).	**Private Cause of Action:** No.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Minnesota Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Minnesota residents. **Important definitions:** *"Security Breach"* means an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. Definition does not include loss of a portable electronic device containing password protected personal information if the encryption key or process is not compromised.	**Subject to statute:** Any person or business doing business in Minnesota that owns or licenses computerized data containing personal information. **Third party recipients:** A covered entity that maintains data that includes personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach immediately following discovery.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. **Other obligations:** Any business that must notify more than 500 persons at one time of a security breach is also required to notify consumer reporting agencies of the security breach within 48 hours.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted and the encryption key, password or other means necessary for reading or using the data has not been acquired. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as the personal information is not used or subject to further unauthorized disclosure. Financial institutions subject to GLBA are exempt. Covered entity deemed in compliance with the Minnesota statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Minnesota statute.		Enforcement under Minn. Stat. §8.31.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Mississippi Click here to review text of statute (*see* Miss. Code, Title 75, § 75-24-29). For specific rules applicable to the insurance industry click here (*See* Miss. Code. Ann. tit. 83 ch 5 art. 11 §§801 *et seq.*) Return to Index of States	**Information covered:** Personal Information of a Mississippi resident. **Important definitions:** "*Security Breach*" means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any Mississippi resident when access to the personal information has not been secured by encryption or by any other method of technology that renders the personal information unreadable or unusable.	**Subject to statute:** Any person who conducts business in Mississippi and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any Mississippi resident. **Third party recipients:** A person that conducts business in Mississippi that maintains computerized data that includes personal information that the person does not own must notify the owner or licensee of the information of any security breach as soon as practicable following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.	**Written, electronic or telephonic notice must be provided** to victims of a security breach without unreasonable delay following completion of an investigation, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice** by means prescribed in the statute if costs to exceed $5,000, affected class exceeds 5,000 persons, or covered entity has insufficient contact information. • **Notice not required if**, after an appropriate investigation, the person reasonably determines that **the breach will not likely result in harm to the affected individuals**.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or otherwise rendered unreadable or unusable.	**A determination of no likelihood of harm:** Does not require notification to Attorney General.	Failure to comply is a violation of state's unfair trade practice.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Missouri Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Missouri residents. Definition includes (i) unique electronic identifier or routing code in combination with required security code, access code or password, (ii) medical information, or (iii) health insurance information. **Important definitions:** *"Security Breach"* means unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the personal information. *"Health Insurance Information"* means an individual's health insurance policy number or subscriber number or any unique identifier used by a health insurer to identify the individual. *"Medical Information"* means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. *"Encryption"* means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. *"Redacted"* means altered or truncated such that no more than five digits of a Social Security Number or the last four digits of a driver's license number, state ID or account number is accessible.	**Subject to statute:** Any person or legal or commercial entity that conducts business in Missouri and that owns or licenses personal information of Missouri residents in any form. **Third party recipients:** Any person that maintains or possesses records or data containing personal information of Missouri residents that the person does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach consistent with the legitimate needs of law enforcement.	**Written, electronic or telephonic notice must be provided** to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • Notice to affected residents is required to contain specific content described in the statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 150,000 persons, or covered entity has insufficient contact information. Substitute notice may also be used for consumers who the covered entity knows to be affected but is not able to identify. • **Notice not required if**, after an appropriate investigation by the covered entity or after consultation with the relevant federal, state or local agencies responsible for law enforcement, the covered entity determines that **a risk of identity theft or other fraud to any consumer is not reasonably likely to occur** as a result of the breach. Such a determination must be documented in writing and retained for five years. **Other obligations:** Any business that must notify more than 1000 persons at one time of a security breach is also required to notify consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise rendered unreadable or unusable. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for a legitimate purpose so long as personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information. Covered entity deemed in compliance with the Missouri statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with Missouri's timing requirements. Any business that complies with the notification procedures imposed by its primary or functional federal or state regulator is deemed in compliance with the Missouri statute.	**Attorney General must be notified if a single breach results in notification to more than 1,000 Missouri residents.** The notice must describe timing, distribution and content of notice to residents. **A determination of no likelihood of harm:** Does not require notification to attorney general. **Other exemptions, cont'd**: Financial institutions are exempt if they are subject to and comply with federal interagency guidelines.	For willful and knowing violations, actual damages and/or civil penalties not to exceed $150,000 for each security breach.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Montana Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Montana residents. Definition includes medical record information, taxpayer identification number, or an identity protection personal identification number issued by the United States internal revenue service. **Important definitions:** *"Security Breach"* means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information and causes or is reasonably believed to cause loss or injury to a person. *"Medical Record Information"* means personal information that: (a) relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment; and (b) is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent or legal guardian. *"Redaction"* means the alteration of personal information contained within data to make all or a significant part of the data unreadable. The term includes truncation, which means that no more than the last four digits of an identification number are accessible as part of the data.	**Subject to statute:** Any person or business that conducts business in Montana and owns or licenses computerized data that includes personal information. (Insurance-support organizations are also covered by Mont. Code §33-19-321.) **Third party recipients:** Any person or business that maintains computerized data containing personal information of Montana residents that the person or business does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach.	**Written, electronic or telephonic notice must be provided** to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • **Notice not required if** covered entity determines that **security breach has not materially compromised the security, confidentiality or integrity of personal information and has not caused or is not reasonably likely to cause loss or injury to a person.** **Other Obligations:** If the notice provided suggests or implies that a consumer can obtain a copy of their file from a credit reporting agency, the business must coordinate with the credit reporting agency regarding the timing, content and distribution of notice to the Montana consumer so long as the coordination does not unreasonable delay the notice to the affected individuals.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of that covered entity so long as personal information is not used or subject to further unauthorized disclosure. Covered entity deemed in compliance with the Montana statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Montana statute.	**Consumer Protection Office of Attorney General must be notified at the same time as notice is provided to affected individuals.** Notice will consist of an electronic copy of the notification to individuals and a statement providing the date and distribution method of the required notification. If notice will be provided to more than one individual, a single copy of the notification must be submitted indicating the number of individuals in the state who received notification. **A determination of no likelihood of harm:** Does not require notification to Attorney General.	Penalties for a violation of the statute are provided in Mont. Code §30-14-142. Temporary and permanent injunctions available.	**Private Cause of Action:** No.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Nebraska Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Nebraska residents. Definition includes (i) unique electronic identification number or routing code in combination with any required security code, access code or password, (ii) unique biometric data, such as fingerprint, voice print, or retina or iris image, or other unique physical representation, and (iii) a user name or email address in combination with a password or security question and answer that permits access to an online account. **Important definitions:** *"Security Breach"* means an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information. *"Redact"* means altering or truncating data in a way that only the last four digits of a social security number, driver's license number, state identification card or account number are accessible. *"Encrypted"* means converted by use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. Data is not considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the security breach.	**Subject to statute:** Individual or commercial entity that conducts business in Nebraska and that owns or licenses computerized data which includes personal information about a Nebraska resident. **Third party recipients:** Any individual or commercial entity that maintains computerized data containing personal information that the individual or commercial entity does not own must notify the owner or licensee of the information of any security breach when it becomes aware of such breach if use of personal information for an unauthorized purpose occurred or is reasonably likely to occur.	**Written, electronic or telephonic notice must be provided** to victims of a security breach as soon as possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $75,000, affected class exceeds 100,000 persons, covered entity has insufficient contact information, or if the covered entity has ten employees or fewer and demonstrates that the cost of providing notice will exceed $10,000. • **Notice not required if**, after a reasonable and prompt investigation, the covered entity determines **there is no reasonable likelihood that the personal information has been or will be used for an unauthorized purpose.**	**Encryption Safe Harbor:** Statute not applicable if the personal data (name or data elements) that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise altered such that the name or data elements are unreadable. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to search warrant, subpoena or court order is not a security breach. Covered entity that maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Nebraska statute is deemed in compliance.	**Attorney General must be notified not later than time when notice is provided to affected residents.** **A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable. **Other exemptions, cont'd:** Any covered entity that complies with the procedures imposed by its primary or functional federal or state regulator is deemed in compliance with the Nebraska statute if it notifies affected residents and the Attorney General in accordance with the maintained procedures in the event of a security breach.	Direct economic damages for each affected Nebraska resident injured by a violation.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Nevada Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Nevada residents when the name and the data elements are not encrypted. Definition includes (i) medical identification number, (ii) health insurance identification number, and (iii) a user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account. **Important definitions:** *"Security Breach"* means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information.	**Subject to statute:** Any institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that handles, collects, disseminates or otherwise deals with nonpublic personal information. **Third party recipients:** Any covered entity that maintains computerized data containing personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • **Notice only required** if security breach materially compromises the security, confidentiality or integrity of personal information. **Other obligations:** Any covered entity that must notify more than 1,000 residents at one time of a security breach is also required to notify consumer reporting agencies of the security breach without unreasonable delay. A business maintaining records which contain personal information concerning customers must take reasonable measures to protect records from unauthorized access and, when they are no longer needed, ensure the destruction of those records in accordance with the statute.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of the covered entity for a legitimate purpose of the covered entity so long as the personal information is not used for a purpose unrelated to the covered entity or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Nevada statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Nevada statute. A covered entity is deemed in compliance with the Nevada statute if it complies with the privacy and security provisions of the GLBA.	**A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Attorney General may bring an action against a covered entity to obtain a temporary or permanent injunction against violations.	**Private Cause of Action:** No. A covered entity that provides the notification required by the Nevada statute may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the covered entity. Damages and restitution relief are available.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
New Hampshire Click here to review text of statute (*see* N.H. Rev. Stat. §359-C:19, *et seq.*) For specific rules applicable to the insurance industry click here. Return to Index of States	**Information covered:** Personal information of New Hampshire. New Hampshire has specific statutes which could apply if an individual's medical information is compromised. **Important definitions:** *"Security Breach"* means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information. *"Encrypted"* means the transformation of data through the use of an algorithmic process into a form for which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements completely unreadable or unusable.	**Subject to statute:** Any person, business, legal entity or governmental entity that conducts business in New Hampshire and owns, maintains or licenses computerized data that includes personal information. **Third party recipients:** Any covered entity that maintains computerized data containing personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach and provide cooperation as needed and required by statute.	**Written, electronic or telephonic notice must be provided** to victims of a security breach as soon as possible. • Notice to affected residents is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $5,000, affected class exceeds 1,000 persons, or covered entity has insufficient contact information. • **Notification is not required if it is determined that misuse of the information has not occurred and is not reasonably likely to occur.** **Other obligations:** Any covered entity that must notify more than 1,000 consumers at one time of a security breach is also required to notify consumer reporting agencies of the security breach without unreasonable delay.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. Data acquired in combination with the required key, security code, access code or password is not considered encrypted. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business so long as personal information is not used or subject to further unauthorized disclosure. Any person engaged in trade or commerce subject to RSA 358-A:3, I which maintains procedures for security breach notification pursuant to a state or federal regulator will be deemed in compliance with the New Hampshire statute. A covered entity is deemed in compliance with the New Hampshire statute if it is subject to the GLBA.	**Attorney General or the primary regulator applicable to covered entity must be notified of a security breach.** Any person engaged in trade or commerce subject to RSA 358-A:3, I must notify the regulator which has primary regulatory over such trade or commerce. All others notify must notify the Attorney General. Notice must include anticipated date of notice to individuals affected and the approximate number of individuals in the state who will be notified. **A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Civil penalties up to $10,000 per violation when actions brought by the Attorney General (injunctive and restitution relief also available). Private citizens injured as a result of violation may bring an action for damages and for equitable relief, including an injunction. Recovery will be actual damages (or up to two to three times actual damages if violation was knowing and willful). A prevailing plaintiff may also be awarded costs and reasonable attorney's fees.	**Private Cause of Action:** Yes. Attorney General and affected residents can enforce.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
New Jersey Clickhere to review text of statute (see N.J. Stat., Title 56, §56:8-161 *et seq.*) Return to Index of States	**Information covered:** Personal information of New Jersey residents. Definition also includes: • Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data. • User name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account. **Important definitions:** *"Security Breach"* means 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 of technology that renders the personal information unreadable or unusable. **Note**: Retail establishments in New Jersey are also regulated by the New Jersey Personal Information and Privacy Protection Act, which governs collection and use of personal information, and provides fines and a private right of action for violations.	**Subject to statute:** Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information. **Third party recipients:** Any covered entity that maintains computerized records containing personal information on behalf of another business or public entity must notify such other business or public entity of any security breach.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • **Notice not required if** the covered entity establishes that **misuse of the information is not reasonably possible**. Such determinations must be documented in writing and retained for five (5) years. Notice for breaches involving user name or password, in combination with any password of security question and answer ONLY (and no other personal information): • Covered entities may provide notification in electronic or other form that directs the consumers whose personal information has been breached to promptly change any password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the business or public entity and all other online accounts for which the consumer uses the same user name or email address and password or security question or answer • Any business or public entity that furnishes an email account shall not provide notification to the email account that is subject to the breach. Notice shall be provided by another method described in the statute or by clear and conspicuous notice	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or secured by any other method or technology that renders the personal information unreadable or unusable. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of covered entity for a legitimate business purpose so long as personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the New Jersey statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the New Jersey statute.	**Division of State Police in the Department of Law and Public Safety must be notified prior to notification to customers.** **A determination of no likelihood of harm:** Does not require notification to Attorney General.		**Private Cause of Action:** No*. *A private cause of action is available under the New Jersey Personal Information and Privacy Protection Act (applies only to retail establishments).

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
New Jersey, cont'd Return to Index of States			delivered to the consumer online when the consumer is connected to the online account from an IP address or online location from which the business or public entity knows the consumer customarily accesses the account. **Other obligations:** Any covered entity that must notify more than 1,000 consumers at one time of a security breach is also required to notify consumer reporting agencies of the security breach without unreasonable delay. Any business or public entity must destroy or arrange for destruction any customer records within its custody or control containing personal information which it no longer needs by shredding, erasing or otherwise modifying the personal information so that it is unreadable, undecipherable or nonreconstructable through generally available means.				

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
New Mexico Click here to review final text of statute. Return to Index of States	**Information covered:** Personal information of New Mexico residents. Definition includes biometric data. **Important definitions:** "*Biometric Data*" means a record generated by automatic measurements of an identified individual's fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account. *"Encrypted"* means rendered unusable, unreadable or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security. *"Security Breach"* means the unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person. "*Service Provider*" means any person that receives, stores, maintains, licenses, processes or otherwise is permitted access to personal identifying information through its provision of services directly to a person that is subject to regulation.	**Subject to statute:** Any person that owns or licenses computerized data that includes personal information. **Third party recipients:** A third party covered entity that maintains computerized data containing personal information that the covered entity does not own or license must notify the owner or licensee of any security breach involving the personal information in the most expedient time possible but not later than forty-five (45) days following determination of the breach unless the third party covered entity concludes, after an appropriate investigation, that the security breach does not give rise to a significant risk of identity theft or fraud..	**Written or electronic notice must be provided** to New Mexico residents whose personal information is reasonably believed to have been subject to a security breach in the most expedient time possible but **not later than forty-five (45) days following the determination of the breach,** unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • Specific content requirements prescribed by statute for notice to individuals. • **Substitute notice is available** by means described in the statute if costs to exceed $100,000, affected class exceeds 50,000 persons, or covered entity has insufficient contact information. • **Notice not required if** the covered entity responsible for the data concludes after a reasonable investigation that **the security breach does not give rise to a significant risk of identity theft or fraud.** **Other obligations:** Any covered entity that must notify more than 1,000 New Mexico residents of a single security breach is also required to notify major consumer reporting agencies in the most expedient time possible but not later than forty-five (45) days following determination of the breach. A covered entity must ensure proper disposal of records containing personal information when they are no longer reasonably needed for business purposes by means of shredding, erasing or otherwise modifying the personal information contained in the records to make it unreadable or undecipherable.	**Encryption Safe Harbor:** Statute not applicable if the personal information that was acquired by an unauthorized individual is encrypted. Safe harbor not available if the confidential process or key is compromised together with the encrypted data. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of covered entity for a legitimate business purpose so long as personal information is not subject to further unauthorized disclosure. A covered entity is deemed in compliance with the New Mexico statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the New Mexico statute. A covered entity that is subject to GLBA or HIPAA is exempt from New Mexico's statute.	**Attorney General must be notified not later than forty-five (45) days after determination of a security breach if more than 1,000 New Mexico residents are affected.** Notification must include the number of New Mexico residents affected and a copy of the notification letter. **A determination of no likelihood of harm:** Does not require notification to Attorney General. **Other obligations, cont'd:** A covered entity must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification or disclosure.	Attorney General may bring action to seek injunctive relief and award of damages for actual costs or losses, including consequential financial losses. If a court determines that a covered entity violated the statute knowingly or recklessly, the court may impose a civil penalty of up to $25,000 or $10.00 per instance of failed notification up to a maximum of $150,000. **Other obligations, cont'd:** A covered entity that discloses personal information of New Mexico residents to a service provider must have a contract in place with the service provider requiring reasonable security procedures and practices appropriate to the nature of the personal information and to	**Private Cause of Action:** No.

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
New Mexico, cont'd						protect it from unauthorized access, destruction, use, modification or disclosure.	
Return to Index of States							

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
New York Click here to review text of statute (*see* N.Y. Gen. Bus. Law, Article 39-F, § 899-AA). Click here to review the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"). [For specific rules applicable to state agencies – *see* N.Y. State Technology Law, §208.] **[For covered entities licensed in New York City** - *see* N.Y. City Admin. Code, Title 20, Chapter 1, §20-117 for additional notification requirements.] [For specific rules applicable to Financial Services Companies – click here.] Return to Index of States	**Information covered:** Private information of New York residents. *"Personal Information"* includes any information concerning a natural person which, because of name, number, personal mark or other identifier can be used to identify such natural person. *"Private Information"* means either: (i) personal information in combination with : • any of the data elements of typical personal information definition; • account number, credit or debit card number, in combination with any required security code, access code, password, **or other information** that would permit access to an individual's financial account; • account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; • biometric information; or (ii) a user name or email address in combination with a password or security question and answer that would permit access to an online account. **Important definitions:** *"Security Breach"* means unauthorized access to or acquisition of, or access to or acquisition without valid authorization of computerized data that compromises the security, confidentiality or integrity of private information maintained by a business.	**Subject to statute:** Any person or business which owns or licenses computerized data which includes private information. **Third party recipients:** Any person or business that maintains computerized data which includes private information which such person or business does not own must notify the owner or licensee of any security breach involving private information immediately following discovery of the breach.	**Written, electronic or telephonic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • Notice to affected residents is required to contain specific content described in statute. • Electronic notice permitted only when the consumer to be notified has consented to such notice, and when such email address, its password, or its security question, was not involved in the breach. A log of all consumers notified electronically must be kept. • **Substitute notice is available** by means prescribed in the statute if a business demonstrates to the state attorney general that costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. **Other obligations:** Any covered entity that must notify more than 5,000 New York residents at one time of a security breach is also required to notify consumer reporting agencies without delaying notice to affected New York residents.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. Safe harbor not available if the compromised data was encrypted with an encryption key that has also been acquired. **Other exemptions:** Exemption for good faith access to, or acquisition of private information by an employee or agent of a business for the purposes of the business so long as any private information is not used or subject to unauthorized disclosure. Notice to consumers not required if exposure to private information was an inadvertent disclosure by persons authorized to access private information, and the business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials. Such determination must be in writing and maintained for 5 years. If incident affects more than 500 NY residents,	**Attorney General and Department of State and Division of State Police must be notified of a security breach without delaying notice to affected residents.** The notification must describe timing, content and distribution of the notices to residents and the approximate number of affected persons, and must include a template of the resident notice. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" to the secretary of health and human services pursuant to HIPAA or HITECH shall provide such notification to the state attorney general within five business days of notifying the secretary.	Injunctive relief available, as well as actual costs or losses incurred by affected residents, including consequential financial losses. For knowing or willful violations, civil penalties of the greater of $5,000 or up to $20 per instance of failed notification, provided that the latter amount may not exceed $250,000.	**Private Cause of Action:** No. Attorney General may bring action on behalf of victims of a security breach within three years of earlier of: (i) date Attorney General became aware of incident; or (ii) date of notice to Attorney General. In no event may an action be brought after six years from the date of discovery of a breach, unless the company took steps to hide the breach.

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
New York, cont'd Return to Index of States	• In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person. • In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person. • Determination whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization can include factors such as: (a) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information, (b) indications that the information has been downloaded or copied, and (c) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of ID theft reported. **Note**: The statute contains a "reasonable security requirement" for businesses that own or license private information of New York residents, the specific requirements of which are contained in the statute.			a written determination must be provided to Attorney General within 10 days of determination. Covered entities that provide notice to consumers of an incident pursuant to the following laws are not required to provide additional notice to consumers under the statute, but are still required to provide notice to the Attorney General, Dept. of State, and Division of State Police: • GLBA • HIPAA/HITECH • HITECH • Regulated financial services companies • Data security rules and regulations of any federal or New York state agency			

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
North Carolina Click here and here to review text of statute. Return to Index of States	**Information covered:** Personal information of North Carolina. Definition includes (i) employer taxpayer identification numbers, (ii) Personal Identification (PIN) Code, (iii) biometric data, (iv) fingerprints, and (v) any other numbers or information that can be used to access a person's financial resources. Personal information does not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources. **Important definitions:** *"Security Breach"* means an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Access to encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. *"Encryption"* means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.	**Subject to statute:** Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form, whether computerized, paper or otherwise. **Third party recipients:** Any business that maintains or possesses records or data containing personal information of North Carolina residents that the business does not own or license must notify the owner or licensee of the information of any security breach immediately following discovery of the breach consistent with law enforcement needs. **Important definitions, cont'd:** *"Redaction"* means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data.	**Written, electronic or telephonic notice must be provided** to victims of a security breach without unreasonable delay, unless a law enforcement agency requests delay in writing due to its determination that notification would impede a criminal investigation or jeopardize national or homeland security (in which case notification is delayed until authorized by law enforcement agency). • Electronic notice allowed only when the consumer to be notified has consented to receipt of electronic communications. • Notice to affected residents is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, covered entity has insufficient contact information, or covered entity is unable to identify particular affected persons. • **Notice not required if** the business responsible for the data concludes that the **security breach is not reasonably likely to cause or create a "material risk of harm" to consumers**. **Other obligations:** Any business that must notify more than 1,000 persons at one time of a security breach is also required to notify consumer reporting agencies without unreasonable delay.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. **Other exemptions:** Exemption for good faith acquisition of personal information by employee or agent of a business for a legitimate purpose so long as personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure. Financial institutions subject to and in compliance with federal interagency guidelines, and credit unions subject to the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, are exempt.	**Consumer Protection Division of Attorney General must be notified of a security breach by a designated online form.** Notification details the nature of the breach, number of affected individuals, the circumstances surrounding the breach, the steps taken to prevent a similar breach in the future, and information about the timing, distribution and content of notice to affected residents. North Carolina Security Breach Reporting Form. **A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Violations fall under G.S.§75-1.1. Civil penalties of up to $5,000 per violation are available under G.S.§75-15.2.	**Private Cause of Action:** Yes, but only if the individual is actually injured as a result of a violation of the statute. Enforcement by Attorney General under G.S.§75.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
North Dakota Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of North Dakota residents. Definition also includes (i) date of birth, (ii) mother's maiden name, (iii) employee identification number in combination with any required access code or password, (iv) electronic or digitized signature, (v) health insurance information, and (vi) medical information. **Important definitions:** *"Security Breach"* means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media or databases unreadable or unusable. *"Health Insurance Information"* means an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. *"Medical Information"* means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.	**Subject to statute:** Any person that owns or licenses computerized data that includes personal information. **Third party recipients:** Any person that maintains or possesses records or data containing personal information that the person does not own or license must notify the owner or licensee of the information of any security breach immediately following discovery of the breach.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. Both the name information and associated data elements must be encrypted. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of the covered entity so long as personal information is not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the North Dakota statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the North Dakota statute. A financial institution, trust company or credit union subject to and in compliance with interagency guidance for unauthorized access to customer information and customer notice is deemed in compliance with North Dakota statute.	**Attorney General must be notified by mail or email if a single breach results in notice to more than 250 individuals.** **Other exemptions, cont'd:** A covered entity subject to HIPAA is deemed in compliance with North Dakota statute.	Remedies for violations are set forth in N.D. Cent. Code 51-15.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Ohio Clickhere to review text of statute. [For specific rules applicable to state agencies – *see* Ohio Rev. Code §1347.12.] [For specific Safe Harbor Requirements – *see* Sec. 1354.02 of the Revised Codes] Return to Index of States	**Information covered:** Personal information of Ohio residents. **Important definitions:** *"Security Breach"* means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted information owned by or licensed to a covered entity and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to person or property. *"Encryption"* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. *"Redacted"* means altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data.	**Subject to statute:** Any person, legal entity or business entity that conducts business in the state that owns or licenses computerized data that includes personal information. **Third party recipients:** Any person that, on behalf of or at the direction of another person or governmental entity, is the custodian of or stores computerized data that includes personal information, must notify that other person or governmental entity of any security breach in an expeditious manner if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to an Ohio resident.	**Written, electronic or telephonic notice must be provided** to victims of a security breach within the most expedient time possible but **no later than forty-five (45) days following the discovery of the breach**, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. **Substitute notice also available to business entities with 10 employees or fewer that demonstrate costs will exceed $10,000.** • **Notification required solely** in the case of breaches that have caused or are reasonably likely to cause a material risk of identity theft or other fraud to an Ohio resident. **Other obligations:** Any covered entity that must notify more than 1,000 Ohio residents at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies without delaying notice to affected Ohio residents.	**Encryption Safe Harbor:** A covered entity may seek an affirmative defense under sections 1354.01 to 1354.05 of the Revised Code by means found in section 1354.02. **Other exemptions:** Exemption for good faith acquisition of personal information or restricted information by the covered entity's employee or agent for the purposes of the covered entity's, provided that the personal information or restricted information is not used for an unlawful purpose or subject to further unauthorized disclosure. A covered entity subject to HIPAA is deemed in compliance with the Ohio statute. A financial institution, trust company or credit union, or any affiliates thereof, subject to and in compliance with information security breach protocols imposed by a functional government regulatory agency, is deemed in compliance with Ohio statute.	**A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Civil penalty of up to $1,000 for each day of non-compliance with statute, up to $5,000 per day after 60 days, and up to $10,000 per day after 90 days.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Oklahoma Clickhere to review text of statute (*see* Okla. Stat., Title 24, §§ 161 to 166). [For specific rules applicable to state agencies – *see* Okla. Stat. §§74-3113.1.] Return to Index of States	**Information covered:** Personal information of Oklahoma residents. **Important definitions:** *"Security Breach"* means unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained as part of a database of personal information regarding multiple individuals and that causes, or the covered entity reasonably believes caused or will cause, identity theft or other fraud to any Oklahoma resident. *"Encrypted"* means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or rendering the data elements unreadable or unusable by other means. *"Redact"* means alteration or truncation of data such that no more than five digits of a social security number or the last four digits of a driver license number, state identification card number or account number are part of the data.	**Subject to statute:** An individual or entity that owns or licenses computerized information that includes personal information. **Third party recipients:** Any covered entity that maintains computerized data containing personal information that the covered entity does not own or license must notify the owner or licensee of the information of any security breach immediately as soon as practicable following discovery of the breach.	**Written, telephonic or electronic notice must be provided** to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information or does not have consent to provide notice otherwise. • **Notification required solely** in the case of breaches that the covered entity reasonably believes has caused or will cause identity theft or other fraud to any Oklahoma resident.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. A breach must also be disclosed if the encryption key is compromise. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Oklahoma statute if it maintains and complies with its own notification procedures as part of an information privacy or security policy and whose procedures are consistent with the timing requirements of the Oklahoma statute. A covered entity that complies with the notification requirements imposed by its primary or functional federal regulator is deemed in compliance with the Oklahoma statute.	**A determination of no likelihood of harm:** Does not require notification to Attorney General. **Other exemptions, cont'd:** Financial institutions subject to and in compliance with federal interagency guidelines are exempt.	Actual damages resulting from a violation of the statute or a civil penalty not to exceed $150,000 per breach. Violations of the statute by state-chartered or state-licensed financial institutions may only be enforced by the primary state regulator of the institution.	**Private Cause of Action:** No. Enforcement by Attorney General or a district attorney.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Oregon Click here to review text of statute (*see* Oregon Rev. Stat. §646A.600 *et seq.*) [For 2018 updates to Oregon Rev. Stat. §646A.600 *et seq* – click here] Return to Index of States	**Information covered:** Personal information of Oregon consumers. Definition includes (i) a passport number or other identification number issued by the United States; (ii) data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction; (iii) a health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or (iv) information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer. Definition also includes a user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification. If data elements have not been encrypted, redacted or rendered unusable and the data element taken would enable a person to commit identity theft, the data element can be considered personal information. **Important definitions:** *"Security Breach"* means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains or possess. *"Encryption"* means an algorithmic process that renders data unreadable or unusable	**Subject to statute:** Any person, legal entity or public body (as defined in ORS 174.019) that owns, or licenses, maintains, stores, manages, collects, processes, acquires **or otherwise possesses** personal information, or that has access to personal information as a consequence of a contract, that the person uses in the course of the person's business, vocation, occupation or volunteer activities. **Third party recipients:** A person that maintains, stores, manages, collects, processes, acquires or otherwise possesses or has access to personal information on behalf of, as a consequence of a contract, or under license of, another person shall notify the other person after discovering a breach of security.	**Written, telephonic or electronic notice must be provided** to victims of a security breach **in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security** unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • Notice to affected residents is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 250,000 persons, or covered entity has insufficient contact information. • **Notice not required if**, after appropriate investigation or consultation with relevant law enforcement authorities, **it is determined that no affected consumers are likely to suffer harm**. Written documentation of this determination is required and must be retained for 5 years. A vendor shall notify the Attorney General in writing or electronically if the vendor was subject to a breach of security that involved the personal information of more than 250 consumers or a number of consumers that the vendor could not determine in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security **Other obligations:** Any covered entity that must notify more than 1,000 Oregon residents at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies without delaying notice to affected Oregon residents.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise rendered unusable by other methods. Safe harbor not available if a security breach involves encrypted data but the encryption key has been compromised. **Other exemptions:** Exemption for good faith and inadvertent acquisition of personal information by a covered entity or a covered entity's employee or agent if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information. A covered entity is deemed in compliance with the Oregon statute if it complies with notification requirements or procedures imposed by its primary or functional federal regulator that are at least as protective as Oregon's statute. Statute not applicable to a covered entity that complies with the Health Insurance Portability and Accountability Act of 1996 and the Health	**Attorney General must be notified electronically or by mail if a single breach affects 250 residents.** **Attorney General must receive within a reasonable time at least one copy of any notice the person sends to consumers or to the person's primary or functional regulator.** **A vendor must notify the Attorney General electronically or by mail if a breach involves more than 250 residents or the number of residents cannot be determined.** **A determination of no likelihood of harm:** Does not require notification to Attorney General. **Other exemptions, cont'd:** A covered entity that complies with other state or federal law that is at least as thorough as Oregon's statute is exempt from Oregon's statute. A covered entity that is subject to GLBA or	Violations are an unlawful practice under ORS 646.607. Penalties can include $1,000 per violation. In the case of a continuing violation, each day's continuance is a separate violation. Maximum penalty of $500,000.	**Private Cause of Action:** No. Enforcement by the Director of the Department of Consumer and Business Services. If the director has reason to believe that any person has engaged or is engaging in any violation of the Oregon statute, the director may issue a cease and desist order, or require the person to pay compensation to consumers injured by the violation. The director may order compensation to consumers only upon a finding that enforcement of the rights of the consumers by private civil action would be so burdensome or expensive as to be impractical.

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Oregon, cont'd Return to Index of States	without the use of a confidential process or key.		Covered entities must develop, implement and maintain **administrative, technical and physical** safeguards to protect personal information. **Note: ORS §654A.22(2)(d) contains expanded information security requirements.** A vendor that discovers a breach of security or has reason to believe that a breach of security has occurred must notify a covered entity with which the vendor has a contract not later than 10 days after discovering the breach.	Information Technology for Economic and Clinical Health Act of 2009 if person information that is subject to the ORS 646A.600 to 646A.628 is also subject to those acts	HIPAA is exempt from Oregon's statute.		

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Pennsylvania Clickhere to review text of statute. Return to Index of States	**Information covered:** Personal information of Pennsylvania residents. **Important definitions:** *"Security Breach"* means unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by a covered entity as part of a database of personal information regarding multiple individuals and that causes, or according to the covered entity's reasonable belief has caused or will cause, loss or injury to any resident of Pennsylvania. *"Encryption"* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. *"Redacted"* means altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number or financial account number is accessible as part of the data.	**Subject to statute:** Any individual or business that maintains, stores or manages computerized data that contains personal information of Pennsylvania residents. **Vendors:** A vendor that maintains, stores or manages computerized data on behalf of a covered entity must provide notice of any breach of the security system following discovery of the breach.	**Written, telephonic or e-mail notice (if a prior business relationship exists) must be provided** to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. • **Notice not required if** the covered entity responsible for the data concludes that the **breach did not cause, or in its reasonable belief has not caused or is not likely to cause, loss or injury to any resident of Pennsylvania.** • **Notice only required** if security breach materially compromises the security, confidentiality or integrity of personal information. **Other obligations:** Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Safe harbor is not available if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key. **Other exemptions:** Exemption for good faith acquisition by an employee or agent of a covered entity for the purposes of the covered entity so long as personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Pennsylvania statute if it maintains and complies with its own notification procedures as part of an information privacy or security policy and whose procedures are consistent with the timing requirements of the Pennsylvania statute.	**A determination of no likelihood of harm:** Does not require notification to Attorney General. **Other exemptions, cont'd:** A covered entity that complies with the notification requirements imposed by its primary or functional federal regulator is deemed in compliance with the Pennsylvania statute. Financial institutions that comply with federal interagency guidelines are deemed in compliance with the Pennsylvania statute.	Violation of the statute constitutes an unfair or deceptive act in violation of the Unfair Trade Practices and Consumer Protection Law.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Rhode Island Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Rhode Island residents when the name and the data elements are not encrypted or are in hard copy, paper format. Definition includes (i) medical information, (ii) health insurance information, and (iii) email address in combination with any required security code, access code, or password that would allow access to an individual's personal, medical, insurance, or financial account. **Important definitions:** *"Security Breach"* means unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information. *"Encrypted"* means the transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Data will not be considered to be encrypted if it is acquired in combination with any key, security code or password that would permit access to encrypted data. *"Health Insurance Information"* means an individual's health insurance policy number, subscriber identification number or any unique identifier used by a health insurer to identify the individual.	**Subject to statute:** Any person or legal commercial entity that stores, owns, collects, processes, maintains, acquires, uses or licenses data that includes personal information. **Third party recipients:** Refer to covered entities subject to statute to determine if a third party recipient of personal information is implicated. A covered entity that discloses computerized unencrypted personal information about a Rhode Island resident pursuant to a contract with a nonaffiliated third party must require by contract that the third-party implement and maintain reasonable security procedures and practices to protect the personal information. **Important definitions, cont'd:** *"Medical Information"* means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional or provider.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible but **no later than forty-five (45) calendar days after confirmation of the breach and ability to ascertain information for notice** unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • Notice to affected residents is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $25,000, affected class exceeds 50,000 persons, or covered entity has insufficient contact information. • **Notification not required if security breach does not pose a significant risk of identity theft.** **Other obligations:** A person or business that owns or licenses computerized unencrypted personal information about a Rhode Island resident must implement and maintain a risk-based information security program that contains reasonable security procedures and practices to protect personal information. Any covered entity that must notify more than 500 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the computerized personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. **Other exemptions:** A covered entity is deemed in compliance with the Rhode Island statute if it complies with notification requirements or procedures imposed by its primary or functional federal regulator in the event of a security breach. A covered entity is deemed in compliance with the Rhode Island statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Rhode Island statute. A covered entity subject to HIPAA is deemed in compliance with Rhode Island's statute. A financial institution, trust company or credit union in compliance with federal interagency guidelines is deemed in compliance with Rhode Island's statute.	**Attorney General must be notified if a single breach affects more than 500 residents.** Notification will include information about timing, content, distribution of notices and approximate number of affected individuals. **A determination of no likelihood of harm:** Does not require notification to Attorney General.	Each reckless violation is a civil violation for which a penalty of not more than $100 per record may be imposed. Each knowing and willful violation is a civil violation for which a penalty of not more than $200 may be imposed.	**Private Cause of Action:** No Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
South Carolina Click here to review text of statute (*see* S.C. Code §39-1-90). [For specific rules applicable to the insurance industry – click here.] Return to Index of States	**Information covered:** Personal information of South Carolina residents. Definition also includes other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely identify an individual. **Important definitions:** *"Security Breach"* means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction or other methods that compromise the security, confidentiality or integrity of the personal information, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident.	**Subject to statute:** A person or legal entity (including cooperative or association) conducting business in South Carolina and owning or licensing computerized data or other data that includes personal identifying information. **Third party recipients:** A person conducting business in South Carolina and maintaining computerized data or other data that includes personal information that the person does not own must notify the owner or licensee of the information of a security breach immediately following discovery of the breach.	**Written, electronic or telephonic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • **Notification only required** when illegal use of the personal data acquired has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. **Other obligations:** Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise rendered unusable or unusable. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of its business so long as personal information is not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the South Carolina statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the South Carolina statute. A financial institution subject to GLBA is exempt. Financial institutions subject to and in compliance with federal interagency guidelines are deemed in compliance with the South Carolina statute.	**Consumer Protection Division of Department of Consumer Affairs must be notified if a single breach affects more than 1,000 residents.** **A determination of no likelihood of harm:** Does not require notification to Attorney General.	Knowing and willful violations subject to an administrative fine in the amount of $1,000 for each affected resident (amount to be decided by Department of Consumer Affairs).	**Private Cause of Action:** Yes. A resident of South Carolina who is injured by a violation may institute a civil action to seek an injunction and to recover damages and attorneys' fees and costs, if successful.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
South Dakota Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of South Dakota residents. Definition includes usernames and passwords, financial information, personal identification numbers ("PINs") or other access codes for financial accounts, medical information, health insurance information, and identification number assigned by an employer in combination with any required security code, access code, password, or biometric data. Also covers "protected information," which includes user name or email address with access code for online accounts, and account number or credit or debit card number, in combination with any access code for financial accounts. **Important definitions:** *"Security Breach"* means the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder. *"Information holder"* means any person or business that conducts business in this state, and that owns or licenses computerized personal or protected information of state residents.	**Subject to statute**: Any person or business that conducts business in South Dakota, and that owns or licenses computerized personal or protected information of residents of South Dakota. **Third party recipients:** Third parties maintaining personal information on behalf of a covered entity must notify covered entity about a breach and cooperate as necessary to allow covered entity to comply with statute. The covered entity must satisfy all further notification obligations under the statute.	**Written or electronic notice must be provided** to victims of a security breach as expeditiously as possible and without unreasonable delay, but **no later than sixty (60) days following the discovery of the breach** unless law enforcement agency determines that disclosure will interfere with a criminal investigation (in which case notification delayed until authorized by law enforcement). Notice to affected residents is required to contain specific content described in statute. • If a delay in notification is prompted by law enforcement needs, notice to affected residents must occur **the notification shall be made not later than thirty (30) days** after the law enforcement agency determines that notification will not compromise the criminal investigation. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • **Notice not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a reasonable likelihood of harm to the consumers whose personal information was acquired**. The determination must be documented in writing and maintained for three years. **Other Obligations:** Any covered entity that must notify more than 250 residents at one time of a security breach is also required to notify the Attorney General and consumer reporting agencies without unreasonable delay.	**Encryption Safe Harbor:** Statute not applicable if the personal information that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. **Other exemptions**: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as the personal information is not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the South Dakota statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Tennessee statute. A covered entity that is subject to GLBA or HIPAA is exempt from South Dakota's statute.	**A determination of no likelihood of harm:** Does not require notification to Attorney General.	In addition to any remedy provided under SD § 37-24-6, violations by non-governmental entities are liable for civil penalties up to $10,000 per day per violation.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Tennessee Clickhere to review text of statute (*see* Tenn. Code, Title 47, §47-18-2107, *et seq.*) Return to Index of States	**Information covered:** Personal information of Tennessee residents. **Important definitions:** *"Encrypted"* means computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2. *"Security Breach"* means unauthorized acquisition of unencrypted computerized data, or encrypted computerized data and the encryption key, by an unauthorized person that materially compromises the security, confidentiality or integrity of personal information. *"Unauthorized Person"* includes an employee of a covered entity who is discovered to have obtained personal information and intentionally used it for an unlawful purpose.	**Subject to statute:** Any person or business that conducts business in Tennessee. **Third party recipients:** Any covered entity that maintains computerized data that includes personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach but **no later than forty-five (45) days** from when the breach became known to third party recipient.	**Written or electronic notice must be provided** to victims of a security breach immediately but **no later than forty-five (45) days following the discovery or notification to covered entity of a security breach**, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement but still must occur within forty-five (45) days after the law enforcement agency's authorization). • If a delay in notification is prompted by law enforcement needs, notice to affected residents must occur **no later than forty-five (45) days** after law enforcement agency determines that notification will no longer compromise its investigation. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • **Notice only required** if security breach materially compromises the security, confidentiality or integrity of personal information. **Other obligations:** Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized person is fully encrypted. Safe harbor not available if the encryption key is compromised together with the encrypted data. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as the personal information is not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Tennessee statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Tennessee statute. A covered entity that is subject to GLBA or HIPAA is exempt from New Mexico's statute.	**A determination of no likelihood of harm:** Does not require notification to Attorney General.	Violations fall under the Tennessee Consumer Protection Act and constitute an unfair or deceptive act or practice affecting trade or commerce.	**Private Cause of Action:** Yes. Residents and business entities injured by a violation may institute a civil action to recover damages as well as injunctive relief.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Texas Click here to review text of statute (*see* Tex. Bus & Com. Code §521.002, *et seq.)* Return to Index of States	**Information covered:** Personal information of Texas residents. (Texas uses the defined term "sensitive personal information.") Definition also includes: (i) information about physical or mental health or condition, (ii) the provision of health care to the individual, or (iii) the payment for the provision of health care to the individual. **Important definitions:** *"Security Breach"* means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of sensitive personal information, including data that is encrypted if the person accessing the data has the key required to decrypt the data.	**Subject to statute:** Any person that conducts business in Texas and owns or licenses computerized data that includes sensitive personal information. **Third party recipients:** A person who maintains computerized data that includes sensitive personal information that the person does not own must notify the owner or license holder of the information of any security breach immediately following discovery of the breach.	**Written or electronic notice must be provided** to victims of a security breach without unreasonable delay and within 60 days of the breach, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • Texas statute allows entities from states other than Texas to provide notice to individuals under the other states' law or under Texas law, provided the other state has regulations that require notification of a breach to affected persons. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. **Other obligations:** Any person that must notify more than 10,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies. Businesses are required to implement and maintain reasonable procedures and incident response plans to protect personal information. Businesses are required to have data destruction security procedures for customer records containing personal information that use methods such as shredding, erasing or otherwise modifying the personal information to make it unreadable or indecipherable.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. Safe harbor not available if personal data is encrypted but the encryption key is compromised by security breach. **Other exemptions:** Exemption for good faith acquisition of sensitive personal information by an employee or agent of the covered entity for the purposes of the covered entity so long as the sensitive personal information is not used or disclosed in an unauthorized manner. A person is deemed in compliance with the Texas statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Texas statute.	**Attorney General must be notified if breach affects at least 250 residents:** Persons required to provide notice of a breach under this section must notify the Attorney General within 60 days of discovery of the breach, if the breach affects at least 250 Texas residents. Notification must contain a description of the nature of the breach, number of residents affected, measures taken, future measures the person will take, and information regarding law enforcement investigation of the breach.	Civil penalty of at least $2,000 but not more than $50,000 for each violation. Failure to take reasonable corrective action to comply with the statute can result in additional penalties of $100 per individual per day of failed or delayed notification, not to exceed $250,000 for a single breach. The Attorney General may also seek injunctive and other equitable relief, as well as reasonable expenses, including attorney's fees, court costs, and investigatory costs.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Utah Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of Utah residents. **Important definitions:** *"Security breach"* means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality or integrity of personal information.	**Subject to statute:** Any person who owns or licenses computerized data that includes personal information concerning a Utah resident. **Third party recipients:** A person who maintains computerized data that includes personal information that the person does not own must notify and cooperate with the owner or licensee of the information of any security breach immediately following discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur.	**Written, telephonic or electronic notice must be provided** to victims of a security breach following a prompt investigation within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • Notice may also be completed by publishing notice of the security breach in a newspaper of general circulation and as required in Utah Code §451-101. • **Notification is only required** if the covered entity determines that misuse of the personal for identity theft or fraud has occurred or is reasonably likely to occur. **Other obligations:** Any person who conducts business in Utah and maintains personal information must implement and maintain reasonable procedures to protect personal information and ensure proper destruction of records containing personal information that no longer need to be retained with methods such as shredding, erasing or otherwise modifying personal information such that it is indecipherable.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or protected by another method that renders the data unreadable or unusable. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a person possessing unencrypted computerized data so long as personal information is not used for an unlawful purpose or disclosed in an unauthorized manner. A person is deemed in compliance with the Utah statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Utah statute. A covered entity is deemed in compliance with the Utah statute if it complies with notification requirements or procedures imposed by its primary or functional federal regulator.	**A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Civil fines no greater than $2,500 per violation or series of violations concerning a specific consumer, and no greater than $100,000 in the aggregate for related violations concerning more than one consumer. Injunctive relief is also available.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Vermont (updated for July 1, 2020 changes) Click here to review text of statute. [For specific rules applicable to data brokers – click here.] Return to Index of States	**Information covered:** Personal information of Vermont residents (referred to as "personally identifiable information"). Definition also includes: • a financial account number or credit or debit card number if the number could be used without additional identifying information, access codes, or passwords; • a password, personal identification number, or other access code for a financial account. • unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; • genetic information; and • (I) health records or records of a wellness program or similar program of health promotion or disease prevention; (II) a health care professional's medical diagnosis or treatment of the consumer; or (III) a health insurance policy number. **Important definitions:** *"Data Collector"* may include the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other	**Subject to statute:** Any Data Collector that owns or licenses computerized personally identifiable information or login credentials. **Third party recipients:** Any Data Collector that maintains or possesses computerized data containing personally identifiable information or login credentials that the Data Collector does not own or license or any Data Collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information or login credentials that the Data Collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement **Note: The statute imposes various obligations on Data Brokers, including, registration, breach record-keeping, and data security requirements. Further specific information is contained in the statute.**	**Written, telephonic or electronic notice must be provided** to victims of a security breach following a prompt investigation within the most expedient time possible and without unreasonable delay, **but not later than forty-five (45) days after discovery of the breach or notification from a third party**, unless a delay is requested by a law enforcement agency concerned that disclosure will impede a law enforcement investigation or a national or homeland security investigation or jeopardize public safety or national or homeland security interests (in which case notification is delayed until authorized by the law enforcement agency). • Electronic notice only permitted under certain conditions. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $10,000, or covered entity has insufficient contact information. • **Notice not required if** covered entity establishes that **misuse of personally identifiable information or login credentials is not reasonably possible and covered entity provides notice of such determination to the Attorney General or the Department of Financial Regulation, as applicable.** **Security Breaches of Login Credentials:** • If a security breach is limited to an unauthorized acquisition of login credentials for an online account other than an e-mail account, consumer notice may be made electronically or through one or more of the methods specified in the statute and shall advise the consumer to take steps necessary to protect the online account, including to change his or her login credentials for the account and for any other account for which the consumer uses the same login credentials.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or protected by another method that renders the data unreadable or unusable. **Other exemptions:** "Security breach" does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the Data Collector for a legitimate purpose of the Data Collector, provided that the personally identifiable information or login credentials are not used for a purpose unrelated to the Data collector's business or subject to further unauthorized disclosure. Financial institutions subject to certain federal interagency guidance regarding consumer information are exempt. Covered entities subject to HIPAA shall be in compliance with security breach notification requirements of the statute with respect to health information is notice is provided to consumers pursuant to HIPAA.	**Attorney General must be notified within fourteen (14) business days of discovery of security breach or notification to consumers, whichever is sooner.** Notice must contain a preliminary description of the breach, the date of the breach, the date of discovery, the number of Vermont consumers affected, and a copy of any notice already provided to consumers. The Data Collector may send to the Attorney General or the Department, as applicable, a second copy of the consumer notice, from which is redacted the type of personally identifiable information or login credentials that was subject to the breach, and which the Attorney General or the Department shall use for any public disclosure of the breach. **For Vermont-regulated financial institution:** Notice must be made to Vermont's Department of Financial Regulation in the same manner as the Attorney General notice.		**Private Cause of Action:** Yes* *a private cause of action may be available to consumers under VT's Consumer Protection Act Enforcement by Attorney General and State's Attorney only. Enforcement by Department of Financial Regulation for regulated financial institutions.

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Vermont, cont'd [Return to Index of States]	entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information. *"Security Breach" m*eans unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality or integrity of a consumer's personally identifiable information or login credentials maintained by a Data Collector. *"Encryption"* means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. *"Redaction"* means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data. *"Login credentials"* means a consumer's user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account **Specific to Data Brokers (2018 Data Broker Regulation):** **Information Covered:** "Brokered personal information": one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties: (i) name; (ii) address;		• If a security breach is limited to an unauthorized acquisition of login credentials for an email account: (A) the data collector shall not provide notice of the security breach through the email account; and (B) the data collector shall provide notice of the security breach through one or more of the methods specified in the statute or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an Internet protocol address or online location from which the data collector knows the consumer customarily accesses the account. **Notice Requirements:** **The notice to a consumer shall be clear and conspicuous. The notice shall include a description of each of the following, if known to the Data Collector:** **(A) the incident in general terms;** **(B) the type of personally identifiable information that was subject to the security breach;** **(C) the general acts of the Data Collector to protect the personally identifiable information from further security breach;** **(D) a telephone number, toll-free if available, that the consumer may call for further information and assistance;** **(E) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and** **(F) the approximate date of the security breach.** **Other obligations:**		A Data Collector who, prior to the date of the breach, on a form and in a manner prescribed by the Attorney General, had sworn in writing to the Attorney General that it maintains written policies and procedures to maintain the security of personally identifiable information or login credentials and respond to a breach in a manner consistent with Vermont law shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers. **Note**: If a security breach is limited to an unauthorized acquisition of login credentials, a data collector is only required to provide notice of the security breach to the Attorney General or Department of Financial Regulation, as applicable, if the login credentials were acquired directly from the data collector or its agent.		

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Vermont, cont'd [Return to Index of States](#)	(iii) date of birth; (iv) place of birth; (v) mother's maiden name; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; (vii) name or address of a member of the consumer's immediate family or household; (viii) Social Security number or other government-issued identification number; or (ix) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty. **Important Definitions:** *"Data Broker"* means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. (note: the statute contains several exemptions) *"Data Broker Security Breach"* means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person.		Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies. **Note**: VT also imposes data destruction requirements pursuant to Vermont's Data Destruction Act, and regulates collection, use and release of Social Security Numbers pursuant to the Social Security Number Protection Act. The applicable statutes contain specific obligations.		**A determination of no likelihood of harm:** Requires notification and detailed explanation to Attorney General. If facts arise later indicating misuse is reasonably possible, the covered entity must notify affected residents. A **waiver** of the statute is void and unenforceable. **Note**: Data Broker Security Breaches do not require Attorney General or Consumer notice unless personal information is involved. However, the statute includes specific record-keeping and reporting requirements.		

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Virginia Click here to review text of statute. [For specific rules applicable to income tax return preparers – click here.] Return to Index of States	**Information covered:** Personal information of Virginia residents. **Important definitions:** *"Security Breach"* means unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to a Virginia resident. *"Encrypted":* Means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable. *"Redact"* means alteration or truncation of data such that no more than five digits of a social security number or the last four digits of a driver's license number, state identification card number, or account number, are accessible as part of the personal information.	**Subject to statute:** Any individual, legal or commercial entity that owns or licenses computerized data that includes personal information. **Third party recipients:** Any covered entity that maintains computerized data that includes personal information that the covered entity does not own or license must notify the owner or licensee of the information of any security breach without unreasonable delay following discovery of the breach.	**Written, telephonic or electronic notice must be provided** to victims of a security breach without unreasonable delay, unless disclosure impedes law enforcement investigation (in which case notification is delayed until authorized by the law enforcement agency). • Notice to affected residents is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information or does not have consent to provide notice by primary means. • **Notice only required if** the security breach causes, or the covered entity **reasonably believes has caused, or will cause, identity theft or other fraud to a Virginia resident.** **Other obligations:** Any person that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies and the Attorney General.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Safe harbor not available if personal information is encrypted but the encryption key is compromised. **Other exemptions:** A covered entity is deemed in compliance with the Virginia statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Virginia statute. A covered entity is deemed in compliance with the Virginia statute if it complies with notification requirements or procedures imposed by its primary or functional state or federal regulator. A covered entity subject to GLBA is deemed in compliance.	**Attorney General must be notified of a security breach.** **A determination of no likelihood of harm:** Does not require notification to Attorney General. Employers or payroll service providers who experience a security breach containing a taxpayer identification number in combination with the income tax withheld **must notify the Department of Taxation** if breach involves payroll information. Notice must include the employer's name and federal employer identification number.	Attorney General may bring an action and may impose a civil penalty not to exceed $150,000 per security breach or a series of breaches of a similar nature that are discovered in a single investigation. Individuals may bring an action to recover direct economic damages resulting from a violation of the Virginia statute.	**Private Cause of Action:** Yes. Enforcement by Attorney General and individuals. Violations by state-charted or licensed financial institutions are redressed by its primary state regulator. Violations by insurance companies are redressed by the State Corporation commission.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Washington Click here to review text of statute. [For specific rules applicable to state agencies – *see* Wash. Rev. Code §42.56.590 *et seq*.] Return to Index of States	**Information covered:** Personal information of Washington residents. Definition also includes a username or email address in combination with a password or security questions and answers that would permit access to an online account, and an individual's first initial and last name in combination with (i) full date of birth, (ii) private key that is unique to an individual and that is used to authenticate or sign an electronic record, (iii) student, military, or passport identification number, (iv) health insurance policy number or health insurance identification number, (v) information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer or (vi) biometric data generated by automatic measurements of an individual's biological characteristics such as fingerprint, voiceprint, retinas, irises, or other unique biological patterns or characteristics. Any of the data elements described above are personal information without the first initial and last name if encryption methods have not been rendered, or the data element would enable a person to commit identify theft. **Important definitions:** *"Security Breach"* means unauthorized acquisition of data (in any form) that compromises the security, confidentiality or integrity of personal information maintained by the person or business. *"Secured" m*eans encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST)	**Subject to statute:** Any person or business that conducts business in Washington and that owns or licenses data (in any form) that includes personal information. **Third party recipients:** Any covered entity that maintains or possess data (in any form) that may include personal information that the covered entity does not own or license must notify the owner or licensee of the information of any security breach immediately following discovery of the breach.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, **but not later than 30 days after discovery of the security breach**, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • Notice to affected residents is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • If the security breach involves personal information including a user name or password, notice may be provided electronically or by email. However, if the security breach involves login credentials of an email account, the person or business must provide notice using another method. • **Notice not required if** the security breach is **not reasonably likely to subject consumers to a risk of harm.** **Other exemptions, cont'd:** A covered entity subject to HIPAA is exempt. Such covered entities will notify the Attorney General in the event of a security breach. Financial institutes subject to federal interagency guidelines are exempt. Such covered entities will notify the Attorney General in the event of a security breach.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is secured (e.g. encryption or redaction). Safe harbor not available if a confidential process, encryption key or other means to decipher the secured information is compromised. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as the personal information is not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Washington statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Washington statute.	**Attorney General must be notified no more than 30 days after the breach was discovered if a single breach results in notification to more than 500 residents.** Notification must be submitted electronically and include the number (or estimate) of affected Washington residents, a list of the types of personal information that were or are reasonably believed to have been the subject of a breach, a time frame of exposure if known, a summary of steps taken to contain the breach, and a sample copy of the notification to consumers. **A determination of no likelihood of harm:** Does not require notification to Attorney General. A **waiver** of the statute is void and unenforceable.	Violations are an unfair or deceptive act in trade or commerce and an unfair method of competition.	**Private Cause of Action:** Yes. Enforcement by Attorney General and individuals.

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Washington, cont'd	standard or is otherwise modified so that the personal information is rendered unreadable, unusable or undecipherable.						
Return to Index of States							

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
West Virginia Click here to review text of statute. Return to Index of States	**Information covered:** Personal information of West Virginia residents. **Important definitions:** *"Security Breach"* means unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the security breach has caused or will cause identity theft or other fraud to any resident of West Virginia. *"Encrypted"* means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key or securing the information by another method that renders the data elements unreadable or unusable. *"Redact"* means alteration or truncation of data such that no more than the last four digits of a social security number, driver's license number, state identification card number or account number is accessible as part of the personal information.	**Subject to statute:** An individual or legal or commercial entity that owns or licenses computerized data that includes personal information. **Third party recipients:** Any covered entity that maintains computerized data that includes personal information that the covered entity does not own or license must notify the owner or licensee of the information of any security breach as soon as practicable following discovery of the breach.	**Written, telephonic or electronic notice must be provided** to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement). • Notice to affected residents is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. • **Notification is only required if** the covered entity reasonably believes **the security breach has caused or will cause identity theft or other fraud to any West Virginia resident.** **Other obligations:** Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Safe harbor not available if personal information is encrypted but the encryption key is compromised. **Other exemptions:** A covered entity is deemed in compliance with the West Virginia statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the West Virginia statute. A covered entity is deemed in compliance with the West Virginia statute if it complies with notification requirements or procedures imposed by its primary or functional federal regulator that are at least as protective as West Virginia's statute. Financial institutions subject to and in compliance with federal interagency guidelines are exempt.	**A determination of no likelihood of harm:** Does not require notification to Attorney General.	Violations constitute an unfair or deceptive act or practice. No civil penalty may be assessed unless the court finds that the defendant has engaged in a course of repeated and willful violations. No civil penalty will exceed $150,000 per breach or series of breaches of a similar nature that are discovered in a single investigation. Violations by financial institutions will be redressed by their primary regulator.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Wisconsin Clickhere to review text of statute. Return to Index of States	**Information covered:** Personal information of Wisconsin residents. Definition includes (i) an individual's DNA data, and (ii) unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.	**Subject to statute:** An entity whose principal place of business is located inside Wisconsin,, or an entity located outside Wisconsin that maintains or licenses personal information in Wisconsin. Includes entities that maintain a depository account for a resident or lends money to a resident. **Third party recipients:** Any entity (other than individuals) that store personal information pertaining to Wisconsin residents that it does not own or license must notify the owner or licensor of the security breach as soon as practicable following discovery of the breach (unless a contractual agreement states otherwise).	**Notice to victims of a security breach within a reasonable time not to exceed forty-five (45) days after discovery of the security breach**, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland security (in which case notification is delayed until authorized by law enforcement). • Notice may be provided by mail or by a method the entity has previously employed to communicate with the affected persons. Upon written request from an affected person, the covered entity must identify the personal information that was acquired. • **Substitute notice is available** by means described in statute if a covered entity cannot with reasonable diligence determine the mailing address of the subject of the personal information compromised. • **Notice not required if the security breach does not create a material risk of identity theft or fraud to the affected persons.** **Other obligations:** Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise altered in a manner that renders it unreadable. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a covered entity if it is used solely for a lawful purpose. Financial institutions regulated by certain federal laws described in the statute are exempt. Entities covered by HIPAA are exempt.	**A determination of no likelihood of harm:** Does not require notification to Attorney General.		**Private Cause of Action:** No.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Wyoming Click here to review text of statute (*see* Stat., Title 40, Chapter 12 §§40-12-501, *et seq.*) Return to Index of States	Personal identifying information about a resident of Wyoming. Definition includes (i) tribal identification card, (ii) federal or state government issued identification card, (iii) shared secrets or security tokens that are known to be used for data based authentication, (iv) username or email address in combination with a password or security question and answer that would permit access to account, (v) a birth or marriage certificate, (vi) medical information, including medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, (vii) health insurance information, including a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claims history, (viii) unique biometric data, including data generated from measurements or analysis of human body characteristics for authentication purposes, and (ix) individual taxpayer identification number. **Important definitions:** *"Security Breach"* means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of Wyoming.	**Subject to statute:** Any individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming. **Third party recipients:** Any covered entity that maintains computerized data that includes personal identifying information that the covered entity does not own or license must notify the owner or licensee of the information of any security breach as soon as practicable following discovery of the breach. **Important definitions, cont'd:** *"Redact"* means alteration or truncation of data such that no more than five digits of any given data element are accessible as part of the personal information.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement). • Notice to affected residents is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $10,000 for Wyoming-based businesses (or $250,000 for out-of-state businesses), affected class exceeds 10,000 persons for Wyoming-based businesses (or 500,000 for out-of-state businesses), or covered entity has insufficient contact information. • **Notice not required if,** after a reasonable and prompt investigation, the covered entity determines that there is **no reasonable likelihood that personal information has been or will be misused.**	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is redacted. **Other exemptions:** Financial institutions regulated by certain federal laws described in the statute are exempt. Any covered entity subject to HIPAA is exempt.	**A determination of no likelihood of harm:** Does not require notification to Attorney General.	Actions in law or equity permitted to ensure compliance with Wyoming statute and to recover damages.	**Private Cause of Action:** No. Enforcement by Attorney General only.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
District of Columbia Click here to review text of statute (*see* D.C.. Code, Title 28, Subtitle II, Chapter 39, Subchapter II, §§28-3851 *et seq.*) Return to Index of States	**Information covered:** Personal information of District of Columbia residents. Definition also includes (i) An individual's first name, first initial and last name, or any other personal identifier, which, in combination with any of the following data elements, can be used to identify a person or the person's information: • Account number, credit card number or debit card number, or any other number or code or combination of numbers or codes, such as an identification number, security code, access code, or password, that allows access to or use of an individual's financial or credit account • medical information; • genetic information and DNA profile; • health insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer that permits access to an individual's health and billing information; • biometric data; and • any combination of data elements listed above, that would enable a person to commit identity theft without reference to the individual's name. Definition also includes: A user name or e-mail address in combination with a password, security question and answer, or other means of authentication, or any combination of data elements listed above that permits access to an individual's e-mail account **Important definitions:** *"Security Breach"* means unauthorized acquisition of computerized or other electronic data or any equipment or device storing such data that compromises the	**Subject to statute:** Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information. **Third party recipients:** Any covered entity who maintains, handles or otherwise possesses computerized or other electronic data that includes personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach in the most expedient time possible following discovery of the breach.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. Notification to individuals must include: • A description of the categories of information that were acquired, or that were reasonably believed to have been acquired; • Contact information for the person or entity issuing the notification, including business address, telephone number, and toll-free telephone number, if maintained; • Notification of a resident's right to obtain a security freeze, including toll-free telephone numbers and addresses for the major consumer reporting agencies; • Toll-free telephone numbers, addresses, and websites for the Federal Trade Commission and the attorney general of the District of Columbia, including steps to take to avoid identity theft; • Offer of theft protection services at no cost for at least 18 months, if it is reasonably believed that a breach involved the Social Security number or tax identification number of a District resident; • Electronic notice directing a person to change their password and/or security question(s), if the breach only affected an online account. **Other obligations:**	**Encryption Safe Harbor:** Acquisition of data that has been rendered secure, including through encryption or redaction of such data, so as to be unusable by an unauthorized third party unless any information obtained has the potential to compromise the effectiveness of the security protection preventing unauthorized access. **Other exemptions:** Covered entities subject to HIPAA or GLBA and provide notice in compliance with HIPAA and GLBA shall be in compliance with security breach notification requirements of the statute with respect to the notification of residents whose personal information is included in the breach. Notice to Attorney General is still required. A covered entity is deemed in compliance with the District of Columbia statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the District of Columbia. statute. Any covered entity subject to GLBA is exempt.	Written notice to the Office of the Attorney General required if the breach affects 50 or more District residents. Notice shall be made in the most expedient manner possible, without unreasonable delay, and in no event later than when notice is provided to individuals. Notice must include: • The name and contact information of the person or entity reporting the breach; • The name and contact information of the person or entity that experienced the breach; • The nature of the breach; • The types of personal information compromised by the breach; • The number of District residents affected by the breach; • The cause of the breach; • Remediation actions taken, including steps to assist District residents; • The date and timeframe of the breach, if known;	Attorney General may recover a civil penalty not to exceed $100 for each violation, the costs of the action, and reasonable attorney's fees. Each failure to provide a District of Columbia resident with notification is a separate violation. Attorney General may also bring petition for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by District of Columbia residents. Any District of Columbia resident may bring a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages may not include dignitary damages, including pain and suffering.	**Private Cause of Action:** Yes. Enforcement by Attorney General and individuals.

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
District of Columbia, cont'd Return to Index of States	security, confidentiality, or integrity of personal information maintained by the person or entity who conducts business in the District of Columbia.		Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies. The statute contains certain data security requirements for entities that own, license, maintain, handle or otherwise possess personal information of D.C. residents, and certain data destruction requirements. The statute also requires covered entities to enter into written agreements with third party service providers that require the service provider to implement and maintain similar security procedures and practices. Entities subject to the security requirements of GLBA or HIPAA are exempt from the statute's data security requirements.	The term "breach of the security of the system" does not include: (i) A good-faith acquisition of personal information by an employee or agency of the person or entity for the purposes of the person or entity if the personal information is not used improperly or subject to further unauthorized disclosure;	• Address and location of corporate headquarters, if outside of the District; • Any knowledge of foreign country involvement; and • A sample of the notice provided to District residents. A **waiver** of the statute is void and unenforceable. **A determination of no likelihood of harm:** Security Breach does not include "acquisition of personal information of an individual that the person or entity reasonably determines, after a reasonable investigation and consultation with the Office of the Attorney General for the District of Columbia and federal law enforcement agencies, will likely not result in harm to the individual."		

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Puerto Rico Click here to review text of statute (*see* Laws of Puerto Rico, Title 10, Subtitle 3, Chapter 310, §4051 *et seq.*) Return to Index of States	**Information covered:** Personal information of Puerto Rico residents. Definition includes (i) names of users and passwords or access codes to public or private information systems, (ii) medical information protected by HIPAA, (iii) tax information, and (iv) work-related evaluations. Mailing and residential addresses are not included in the definition. **Important definitions:** *"Security Breach"* means any situation in which it is detected that access to personal information has been permitted to unauthorized persons or entities so that the security, confidentiality or integrity of the information has been compromised; or, when those persons authorized to access personal information may have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. The definition includes both physical and electronic intrusions.	**Subject to statute:** Any entity that is the proprietor or custodian of a database that includes personal information of citizen residents of Puerto Rico. **Third party recipients:** Any entity that as part of its operations resells or provides access to digital data banks that at the same time contain personal information files of Puerto Rico citizens must notify the proprietor, custodian or holder of the information of any security breach.	**Written direct notice or authenticated electronic notice must be provided** to victims of a security breach as expeditiously as possible, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • Notice to affected persons is required to contain specific content described in statute. • **Substitute notice is available** by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. Substitute notice may be available in other situations if notification is unduly onerous or difficult.	**Encryption Safe Harbor:** Statute only applies to data that is not protected by a special cryptographic code.	**Department of Consumer Affairs must be notified of any security breach within ten (10) days of detection of security breach.** The Department will make a public announcement about security breach within 24 hours of receiving notification from the covered entity.	Fines of $500 up to a maximum of $5000 for each violation.	**Private Cause of Action:** Yes. Consumers may bring actions in a competent court for damages.

MINTZ

State / Link to Statute	Information Covered / Important Definitions	Covered Entities[1] / Third Party Recipients	Notice Procedures & Timing / Other Obligations	Encryption Safe Harbor / Other Exemptions	Notification to Regulator / Waiver	Penalties	Private Cause of Action / Enforcement
Virgin Islands Click here to review text of statute (*see* V.I. Code, Title 14, Chapter 110, Subchapter I, §2209 *et seq.*) Return to Index of States	**Information covered:** Personal information of Virgin Islands residents. **Important definitions:** *"Security Breach"* means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the covered entity.	**Subject to statute:** Any person or business that conducts business in the Virgin Islands, and that owns or licenses computerized data that includes personal information. **Third party recipients:** Any covered entity that maintains computerized data that includes personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach.	**Written or electronic notice must be provided** to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • **Substitute notice is available** by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 50,000 persons, or covered entity has insufficient contact information.	**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of the covered entity for the purposes of the covered entity so long as the personal information is not used or subject to further unauthorized disclosure.	A **waiver** of the statute is void and unenforceable.	Businesses that violate the statute may be enjoined. Customers injured by a violation may commence a civil action to recover damages.	**Private Cause of Action:** Yes.