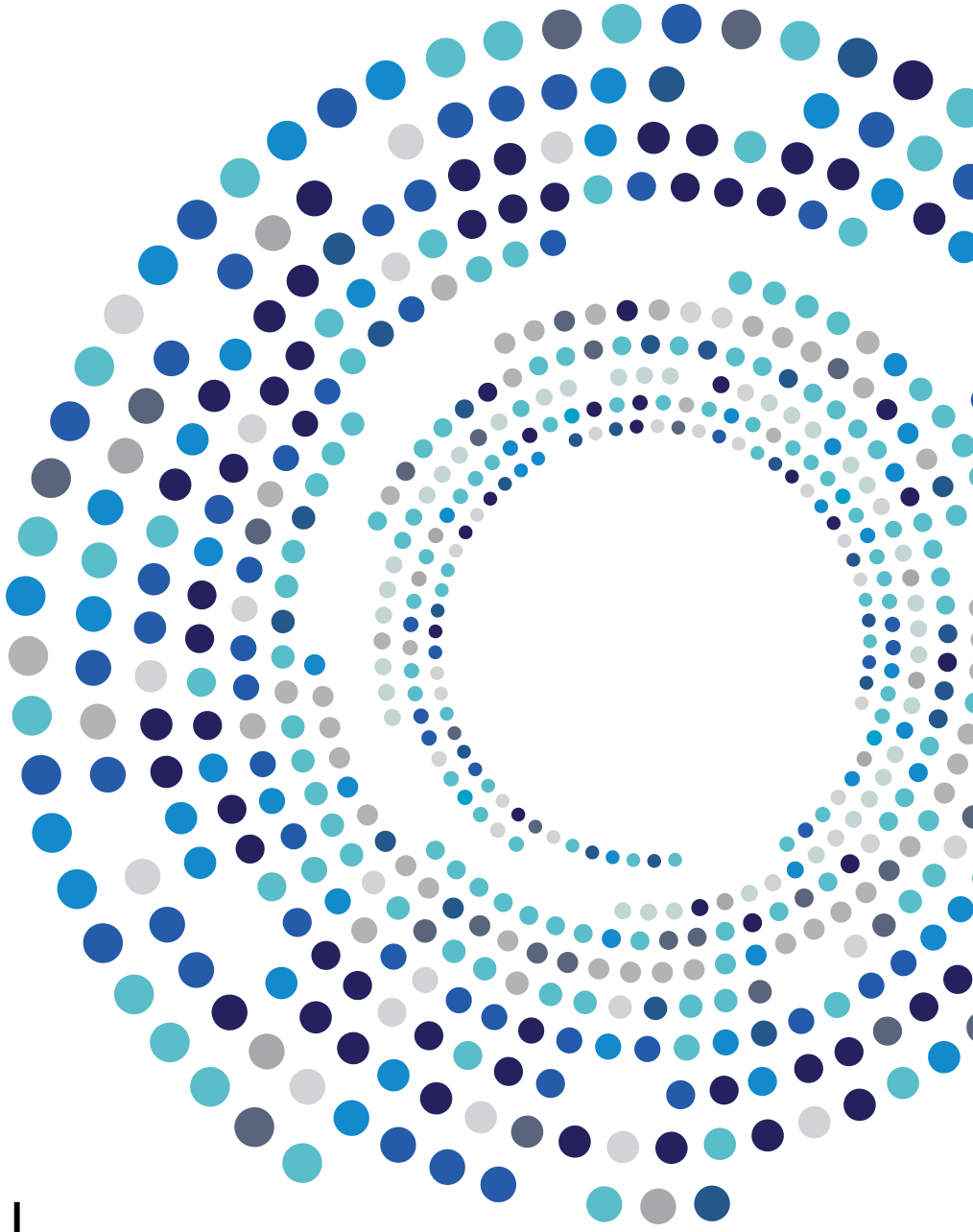
O'Melveny | omm.com



A Guide to US Breach Notification Laws

In a world where one wrong click can compromise a company's data and its customers' privacy, every organization needs a cybersecurity plan—before, during, and after any damage is done.

Our lawyers help clients across the entire life cycle of their data security and privacy concerns, from counseling to policy formation to incident management to the most sensitive negotiations with law enforcement and regulatory agencies at home and abroad. Should data breaches result in class-action litigation or regulatory proceedings, our award-winning litigation and investigations lawyers draw on their decades of success in and out of court to chart the most favorable path forward. O'Melveny's team includes lawyers who have previously tackled these issues at the highest level of government, including:

- US Homeland Security and Counterterrorism Advisor
- General Counsel at the US Department of Homeland Security
- Deputy Legal Advisory at the National Security Council
- Several top lawyers in the DOJ, SEC, and DHS

We are pleased to present this guide to the current legislative landscape around data breach notification by state and territory, including positions on covered entities, definition of personal information, definition of breach, threshold for notification, and other key components of current statutes. [This is an interactive document; use the *Contents by State and Territory* and *Contents by Topic* menus on the following pages to navigate the guide.]

KEY CONTACTS

Steve Bunnell
Co-Chair,
Data Security and Privacy Practice
Washington, DC
+1 202 383 5399
sbunnell@omm.com

Lisa Monaco
Co-Chair,
Data Security and Privacy Practice
Washington, DC: +1 202 383 5413
New York: +1 212 326 2000
lmonaco@omm.com

Randy Edwards
Partner
San Francisco
+1 415 984 8716
redwards@omm.com

Scott Pink
Special Counsel
Silicon Valley
+1 650 473 2629
spink@omm.com

John Dermody
Counsel
Washington, DC
+1 202 383 5306
jdermody@omm.com

Contents by State and Territory

Contents by Topic

CONTENTS BY TOPIC

CONTENTS BY TOPIC

Alabama

State and Statute	Alabama S.B. 318
Covered Entities	Persons, sole proprietorships, partnerships, government entities, corporations, nonprofits, trusts, estates, cooperative associations, third-party agents or other business entities that acquire or use sensitive personally identifying information. Government entities are subject to the Act as well and must provide notice in line with the provisions of the law.
Definition of Personal Information	Information containing an Alabama resident's first name or first initial and last name and one or more of the following: • Social Security number • Driver's license number • Tax identification number • Passport number • Military identification number • Government or State issued unique identification number • Financial account number, credit card number, debit card • Any information regarding the individual's medical history, mental or physical condition, or medical treatment or diagnosis • Health insurance policy number • A username or email address in combination with a password or security question and answer for an account that is reasonably likely to contain personal information *Exceptions:* • Encrypted or redacted information (in a way that removes elements that identify the person or if they make the information unusable). • Information regarding the individual lawfully made public by federal, state, or local government record, or widely distributed media
Definition of Breach	An 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. *Exceptions:* • Good-faith acquisition of sensitive personally identifying information by an employee or agent of an Entity is not a security breach, so long as the information is not used for a purpose unrelated to the business or subject to further unauthorized use. • Release of a public record not otherwise subject to confidentiality or nondisclosure requirements. • Any lawful, investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state.

ALABAMA

Threshold for Notification	When sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person without valid authorization, and the information is reasonably likely to cause substantial harm to the individuals to whom the information relates.
Notification of Data Subject	Yes, if it is reasonably likely to cause substantial harm to an AL resident. Third Parties must notify if covered entity maintains, stores, processes, or otherwise accesses covered information on behalf of another entity, the entity must notify them as expeditiously as possible and without unreasonable delay, but not later than 10 days following discovery of a breach or reason to believe a breach occurred.
Notification of Government	If the number of affected individuals exceeds 1,000, the Entity must notify the Attorney General. Notice should be given as expeditiously as possible and without unreasonable delay, and within 45 days from the date it is determined that a breach has occurred and is reasonably likely to cause substantial harm to such affected individuals.
Notification of Credit Reporting Agencies	Consumer reporting agencies must be informed without unreasonable delay if the breach exceeds 1,000 individuals and is likely to cause substantial harm to the affected individuals.
Notification by Third Parties	—
Timing of Notification	Notice to individuals shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation. The covered entity shall provide notice within 45 days of the covered entity's receipt of notice from a third-party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates. *Exception:* Law Enforcement notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or national security, and the law enforcement agency has submitted a written request for the delay. The relevant agency may revoke the delay as of a specified date or extend the delay, if necessary.

Form of Notification	Notice must be given in writing by either mail or email, describing 1) date, estimated date, or date range of the breach, 2) personally identifying information breached, 3) general descriptions of the actions taken by the covered entity in response to the breach, 4) general description of steps individual can take to protect themselves, 5) information the individual can use to contact the covered entity about the breach. *Exceptions:* Excessive cost, either relative to the resources of the entity or exceeding $500,000; lack of sufficient contact information; or affected individuals exceeding 100,000 persons. *Substitute notice:* Publication on company website for 30 days (in a conspicuous location) and notice to major print and broadcast media in the affected area.
Exemptions or Safe Harbors	Any Entity that is subject to or regulated by state or federal laws, rules, regulations, procedures, or guidance is exempt as long as that Entity: Maintains procedures pursuant to those requirements; provides notice to consumers pursuant to those requirements; and timely provides notice to the Attorney General when the number of affected individuals exceeds 1,000.
Consequences of Non-Compliance	*Government enforcement?* A violation of the notification provisions of this act is an unlawful trade practice, but does not constitute a criminal offense. Any covered entity or third-party agent who is knowingly engaging in or has knowingly engaged in a violation of the notification provisions of this act will be subject to the penalty provisions. A covered entity that violates the notification provisions of this act shall be liable for a civil penalty of not more than five thousand dollars ($5,000) per day for each consecutive day that the covered entity fails to take reasonable action to comply with the notice provisions of this act. *Private right of action?* No
Credit Monitoring Required	—

Alaska

State and Statute	Alaska Stat. § 45.48.010 et seq.
Covered Entities	Any person, state, or local governmental agency, or an entity with more than 10 employees that owns or licenses personal information in any form in AK that includes PI of an AK resident. *Exceptions:* Judicial agencies; individuals with less than ten employees.
Definition of Personal Information	Information containing an individual's full name and one or more of the following: Information in any medium on an individual that is not encrypted or redacted, and that consists of a combination of an individual's first name or first initial and last name in combination with any one or more of the following data elements: • Social Security number • Driver's license number • State issued identification card number • Passport number • Military identification number • Credit card, debit card, and/or bank account number • Information necessary to access financial accounts (including but not limited to passwords and PIN numbers) *Exceptions:* Encrypted or redacted information not including encrypted information to which the encryption key has been accessed or acquired.
Definition of Breach	An unauthorized acquisition (or reasonable belief of unauthorized acquisition) of personal information that compromises the security, confidentiality, or integrity of the personal information. Acquisition includes acquisitions by photocopying, facsimile, or other paper-based method, by a device that can read, write, or store information represented in numerical form, or other method. *Exceptions:* Good-faith acquisition of personal information by an employee or agent of the information collector for a legitimate purpose is not considered a breach of the security of the information system, provided the personal information is not used for a purpose other than an authorized purpose and is not subject to further unauthorized disclosure.
Threshold for Notification	When the breach is likely to cause "reasonable" harm to the residents of the state whose personal information was compromised.

Notification of Data Subject	Any Entity to which the statute applies shall disclose the breach to each AK resident whose personal information was subject to the breach after discovering or being notified of the breach. *Exceptions:* Notification is not required if, after an appropriate investigation and after written notification to the state Attorney General, the Entity determines that there is no reasonable likelihood of harm to the affected consumers. The determination shall be documented in writing and the documentation shall be maintained for five years.
Notification of Government	—
Notification of Credit Reporting Agencies	Credit Agency must be notified if more than 1,000 residents of the state must receive notification. *Exceptions:* Entities subject to the Gramm-Leach-Bliley Act are exempt from this requirement.
Notification by Third Parties	Third Party must notify if covered entity maintains covered information on behalf of other entity as soon as possible and without delay.
Timing of Notification	Notifications must be sent in the most expeditious way possible and without unreasonable delay. *Exception:* If a government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation

Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing: sent via mail to the most recent address of the affected entity. • Electronically: if the affected entity's preferred method of communication with the information collector is via electronic means or if the method and content of electronic communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act. • Via telephone: if the affected entity's preferred method of communication with the information collector is via telephone. The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $150,000 • The number of affected entities exceeds 300,000 • Contact information for affected entities is unavailable • Prior efforts to contact affected entities were unsuccessful *Alternate forms of notification:* • Email the affected entity if an email address is available • "Conspicuously" post disclosure on the information collector's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* No. *Following agency guidelines?* No. Private right of action against non-government entities.
Consequences of Non-Compliance	*Government enforcement?* Information collectors may be liable for up to $500 for each affected entity who was not notified or notified properly. Total civil penalty may not exceed $50,000. *Private right of action?* Affected entities may bring a civil suit if a non-governmental agency's practices were unfair or deceptive under Alaska law. Damages are limited to economic damages that do not exceed $500.
Credit Monitoring Required	—

Arizona

State and Statute	Arizona Rev. Stat. § 44-7501
Covered Entities	Individuals who conduct business in Arizona and own or have the license to computerized data (including personal information) that is not encrypted.
Definition of Personal Information	Information containing an individual's first name or first initial and last name and one or more of the following: • Social Security number • Driver's license number or non operating identification license number • Credit card, debit card, and/or bank account number • Private key unique to an individual that is used to authenticate or sign an electronic record • Health insurance number • Any information regarding the individual's medical history, mental or physical condition, or medical treatment or diagnosis • Passport number • Taxpayer identification number • Unique biometric data for body characteristics • Information necessary to access financial accounts (including but not limited to passwords and PIN numbers) • A username or email address in combination with a password or security question and answer for an account that is reasonably likely to contain personal information *Exception:* Any information about an individual made public by the federal, state, and/or local government.
Definition of Breach	An unauthorized and unreasonable retrieval of computerized data that "compromises the security or confidentiality" of personal information. Retrieval must cause or risk "substantial economic loss." *Exception:* If the personal information was retrieved in good faith by the employee or agent of the person.
Threshold for Notification	When the covered entity discovers unauthorized and unreasonable retrieval of computerized, unencrypted data, and the covered entity conducts a "reasonable investigation" and determines that there has been a breach.

Notification of Data Subject	Any Entity that owns or licenses the affected personal information shall notify the affected persons within 45 days after determination that there has been a security breach. *Exceptions:* An Entity is not required to disclose a breach of the system if a reasonable investigation, determines that a breach has not resulted in or is not reasonably likely to result in substantial economic loss to the affected persons.
Notification of Government	Attorney General if the breach exceeds 1,000 individuals.
Notification of Credit Reporting Agencies	Consumer reporting agencies if the breach exceeds 1,000 individuals.
Notification by Third Parties	Third Party must notify if covered entity maintains unencrypted computerized data that includes covered information on behalf of another entity.
Timing of Notification	Entity must notify within 45 days after the Entity's determination that there has been a security breach. *Exception:* If a government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Electronically: if the affected entity's preferred method of communication with the information collector is via electronic means • Via telephone: if the person can be reached directly, not via voicemail The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $50,000 • The number of affected entities exceeds 100,000 • Contact information for affected entities is unavailable *Substitute notice:* Email to the individual(s) (if available), publication on company website, and notice in print and broadcast media.

Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's requirements and so long as the covered entity notifies individuals in conjunction with its procedures. *Following agency guidelines?* Yes, so long as the covered entity follows procedures set forth by its primary financial regulator. *Exception:* HIPAA-covered entities.
Consequences of Non-Compliance	*Government enforcement?* Yes. Arizona's attorney general may bring suit "to obtain actual damages" and a civil penalty that does not exceed $10,000 per breach or per similar breaches discovered in a single investigation. Covered entities must "willfull[y]" and "knowing[ly]" violate notification procedures to be liable. *Private right of action?* No.
Credit Monitoring Required	—

Arkansas

State and Statute	Arkansas Code Ann. § 4-110-101 et seq.
Covered Entities	Individuals and businesses that own, license, and/or acquire personal information in the form of computerized data. Businesses are defined as entities "that destroy records" and state agencies.
Definition of Personal Information	Information containing an individual's name and one or more of the following: • Social Security number • Driver's license number • Credit card, debit card, and/or bank account number in combination with information necessary to access financial accounts (including but not limited to passwords and PIN numbers) • Information regarding an individual's medical history, medical records, and/or prior diagnoses • Biometric data or unique biological information *Exception:* Any information about an individual made public by the federal, state, and/or local government.
Definition of Breach	An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an Entity. *Exception:* Good-faith acquisition of personal information An Entity must retain a copy of the determination of the breach and any supporting documentation for five years from the date the breach was determined.
Threshold for Notification	When a covered entity discovers or has reason to believe that unencrypted personal information has been retrieved by an unauthorized individual, and the covered entity conducts an investigation and determines there is reasonable likelihood of harm to customers.
Notification of Data Subject	Yes. Third party must notify if covered entity maintains covered information on behalf of other entity as soon as possible and without delay.
Notification of Government	Attorney General if the breach exceeds 1,000 individuals. Notice must be provided at the same time the Entity notifies the affected class, or 45 days after it determines there is a reasonable likelihood of harm to individuals, whichever is first.
Notification of Credit Reporting Agencies	—

Notification by Third Parties	—
Timing of Notification	Notifications must be sent in the most expeditious way possible and without unreasonable delay. *Exception:* If a government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Electronically in compliance with the E-Sign Act The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 • Contact information for affected entities is unavailable *Substitute notice:* Email to the individual(s) (if available), publication on company website, and notice in print and broadcast media.
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's requirements and so long as the covered entity notifies individuals in conjunction with its procedures. *Following agency guidelines?* Yes, so long as the covered entity follows procedures set forth by its primary financial regulator and so long as the regulator "provides greater protection" or "as thorough disclosure requirements" for breaches as Arkansas's statute does.
Consequences of Non-Compliance	*Government enforcement?* Yes; all violations of Arkansas's notification procedures are "punishable by action" of the state's attorney general. The attorney general must follow state procedures and policies set forth to regulate deceptive trade practices. *Private right of action?* No.
Credit Monitoring Required	—

California

State and Statute	California Civ. Code § 1798.29 [regulating agencies], 1798.80 et seq. [regulating individuals and businesses], 1280.15 [regulating breaches of medical information] California Civ. Code § 1798.80 California Health and Safety Code § 1280.15
Covered Entities	Individuals, businesses, and agencies that own or license personal information in the form of computerized data. A business is defined as a sole proprietorship, partnership, corporation, association, or other group, however organized to operate at a profit. Businesses include entities that dispose of records. Applicable to any Entity maintaining information on CA residents, whether or not the Entity conducts business in CA. Definition expanded as of January 1, 2014, to include medical clinics, health facilities, hospitals, and home health facilities.
Definition of Personal Information	Information containing an individual's name and one or more of the following: • Social Security number • Driver's license number or California identification number • Credit card, debit card, and/or bank account number in combination with information necessary to access financial accounts (including but not limited to passwords and PIN numbers) • Information regarding an individual's medical history, medical records, and/or prior diagnoses • Information necessary to access health insurance account information, such as a policy number or subscription identification number AB 1130 expanded personal information to: • tax identification number • passport number • military identification number • other unique identification numbers issued on a government document commonly used to verify the identity of a specific individual • unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual (does not include a physical or digital photograph unless used or stored for facial recognition purposes) *Exceptions:* Any information about an individual made public by the federal, state, and/or local government.

Definition of Breach	An unauthorized acquisition of computerized data that "compromises the security, confidentiality, or integrity" of personal information. See Cal. Civ. Code § 1798.82(g). Includes the "unlawful or unauthorized access to, and use or disclosure of, patients' medical information." See Cal. Civ. Code § 1280.15(a). *Exception:* Good-faith acquisition of personal information.
Threshold for Notification	Notification Threshold: when a covered entity discovers or has reason to believe that unencrypted personal information has been retrieved by an unauthorized individual. Medical entities must "report any unlawful or unauthorized access to, or use or disclosure of, patients' medical information." See id. at § 1280.15(a). California's Office of Privacy Protection offers nonbinding guidelines for determining whether a breach requires notification. They are as follows: Determine that personal information is in "the physical possession and control of an unauthorized person," such as "a lost or stolen computer." Determine that the personal information has been downloaded or copied by an unauthorized individual. Determine that the personal information has been used by an unauthorized individual, such as to open a "fraudulent account."
Notification of Data Subject	Yes, so long as the covered entity and/or a law enforcement agency determines that the breach has occurred or is likely to occur. AB 1130 Require private actors to provide affected individuals whose biometric data has been breached with information on how to notify other entities that authenticate accounts with the same type of biometric data that they can no longer rely on that data.
Notification of Government	If an Entity is required to notify more than 500 CA residents, the Entity shall electronically submit a single sample copy of the notification, excluding any personally identifiable information, to the Attorney General.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Third party must give notice if covered entity maintains covered information on behalf of other entity as soon as possible and without delay.

Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay. *Exception:* If a government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation. California's Office of Privacy Protection offers nonbinding guidelines for determining the right timeframe for notification. Notification of breach should be provided no later than ten business days after the entity determines that personal information was retrieved or likely was retrieved by an unauthorized individual.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing: in plain language • Electronically: if the method and content of communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 • Contact information for affected entities is unavailable • Prior efforts to contact affected entities were unsuccessful *Alternate forms of notification:* • Email the affected entity if their email address is available. • Conspicuously disclose information on the covered entity's website for a minimum of 30 days. The link should be on the Home/First page and in larger/contrasting font. • Notify major statewide media and notify the Office of Information Security within the Department of Technology.

Exemptions or Safe Harbors	Health care and medical services providers "regulated by the Confidentiality of Medical Information Act." Health care and medical services providers "governed by the medical privacy and security rules" established under the Health Insurance Portability and Availability Act of 1996 (HIPAA), and administered by the US Department of Health and Human Services. Financial institutions "as defined in" the California Financial Code and "subject to" the California Financial Information Privacy Act. Entities "that obtain information under an agreement" under the confidentiality requirements of the California Vehicle Code.
Consequences of Non-Compliance	*Government enforcement?* Yes. *Private right of action?* Yes, private individuals injured by an entity's failure to follow notification procedures may "recover damages." See § 1798.84(b). For private individuals whose medical information is breached: • Covered entities may be subject to civil penalties of up to $25,000 per patient whose medical information is breached, and $17,500 per additional occurrences. • Covered entities may be liable for civil penalties of $100 per day for each day notification is delayed. • Covered entities may be subject to no more than $250,000 in civil penalties for breach of medical information. **California Consumer Privacy Act of 2018** Any consumer whose non-encrypted or non-redacted personal information is breached as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: • To recover damages in an amount not less than one hundred dollars ($100) but not greater than seven hundred and fifty dollars ($750) per consumer per incident or actual damages, whichever is greater. • Injunctive or declaratory relief. • Any other relief the court deems proper.

Consequence of Non-Compliance	Actions pursuant to this section may be brought by a consumer if all of the following requirements are met: • Prior to initiating any action for statutory damages, a consumer shall provide a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement. • A consumer bringing an action for relief other than injunctive or declaratory relief shall notify the Attorney General within 30 days that the action has been filed. The Attorney General, upon receiving a notice of action from a consumer shall, within 30 days, do one of the following: • Notify the consumer bringing the action of the Attorney General's intent to prosecute an action against the violation. If the Attorney General does not prosecute within six months, the consumer may proceed with the action. • Refrain from acting within the 30 days, allowing the consumer bringing the action to proceed. • Notify the consumer bringing the action that the consumer shall not proceed with the action. Note that AB-1130 amends the data breach notification statute that applies to private actors (Cal. Civ. Code § 1798.82) and the state and local agency statute (Cal. Civ. Code § 1798.29). AB-1130's expansion of the personal information definition will also expand the related coverage scope for the CCPA's private right of action.
Credit Monitoring Required	Credit Monitoring Required for 12 months if breach included SSN.

Colorado

State and Statute	Colorado Rev. Stat. § 6-1-716 (Pg. 54)
Covered Entities	A person, including any private legal entity, whether for-profit or not-for-profit, that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. Entity does not need to conduct business in CO. *Exceptions:* Third-party service provider: an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity.
Definition of Personal Information	Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: • Social Security number • Student, military, or passport identification number • Driver's license number or identification card number • Medical information • Health insurance identification number • Biometric data 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; or Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account. *Exception:* Publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.
Definition of Breach	An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. *Exceptions:* Good-faith acquisition of personal information by an employee or agent of a covered entity for the covered entity's business purposes is not a security breach if the personal information is not used for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure.

Threshold for Notification	A covered entity that maintains, owns, or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware that a security breach may have occurred, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused.
Notification of Data Subject	Yes, and third party must give notice if covered entity maintains covered information on behalf of other entity and if misuse of information of a resident has occurred or is reasonably likely to occur.
Notification of Government	If notice is provided to more than 500 CO residents, the Entity must provide notice to the Attorney General, no later than 30 days after the date of determination that the breach occurred.
Notification of Credit Reporting Agencies	If personal information for more than 1,000 Colorado residents has been breached, Commercial entities are required to disclose to credit reporting agencies "the anticipated date of the notification to the residents and the approximate number of residents who are to be notified."
Notification by Third Parties	—
Timing of Notification	Notice must be made in the most expeditious time possible and without unreasonable delay, but no later than thirty 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.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written notice to the postal address listed in the records of the covered entity • Telephonic notice • Electronic notice, if a primary means of communication by the covered entity with a Colorado resident is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the federal "Electronic Signatures in Global and National Commerce Act" The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 250,000 • Contact information for affected entities is unavailable

Form of Notification	*Alternate forms of notification* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's "timing requirements" and so long as the entity notifies individuals in conjunction with its procedures. *Following agency's guidelines?* Yes, so long as the covered entity follows procedures set forth by its primary financial regulator.
Consequences of Non-Compliance	*Government enforcement?* Yes, at the discretion of Colorado's attorney general. The attorney general may seek "relief … appropriate to ensure compliance with this section or recover direct economic damages resulting from a violation, or both." *Private right of action?* No
Credit Monitoring Required	—

Connecticut

State and Statute	Connecticut Gen. Stat. § 36a-701b
Covered Entities	Individuals who conduct business in Connecticut and own, maintain, or license personal information in the form of computerized data.
Definition of Personal Information	Information containing an individual's name and one or more of the following: • Social Security number • Driver's license number or State identification number • Credit card, debit card, and/or bank account number in combination with information necessary to access financial accounts (including but not limited to passwords and PIN numbers) *Exceptions:* Any information about an individual made public by the federal, state, and/or local government.
Definition of Breach	An unauthorized access to or unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information that is not encrypted or protected in a manner that would render it unreadable or unusable.
Threshold for Notification	When the breach is likely to cause reasonable harm to the residents of the state whose personal information was compromised. *Exceptions:* If the personal information was retrieved in good faith.
Notification of Data Subject	Yes. Any Entity to which the statute applies shall disclose any breach of security following the discovery of the breach to any CT resident whose personal information was breached, or is reasonably believed to have been breached.
Notification of Government	Yes, to Connecticut's attorney general; notice must be provided no later than it is provided to residents of the state.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Third party must give notice if covered entity maintains covered information on behalf of other entity as soon as possible and without delay.

Timing of Notification	Notifications must be sent "without unreasonable delay," but no later than 90 days after breach. *Exceptions:* If a government agency determines that disclosure will disrupt a criminal investigation, then a covered entity may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Via telephone • Electronically: if the method and content of communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 • Contact information for affected entities is unavailable *Alternate forms of notification:* • Email the affected entity if email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media, including newspapers, radio, and television
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's "timing requirements" and so long as the entity notifies individuals and the state's attorney general in conjunction with its procedures. *Following agency guidelines?* Yes, so long as the covered entity follows procedures set forth by its primary financial regulator. If notice is given to a CT resident, the Attorney General is notified at the same time.
Consequences of Non-Compliance	*Government enforcement?* Yes, failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General. The AG may seek direct damages and injunctive relief. *Private right of action?* No.
Credit Monitoring Required	Credit Monitoring Required for 24 months if breach included SSN.

Delaware

State and Statute	Delaware Code Ann. Tit. 6, § 12B-101 et seq.
Covered Entities	Any individual, corporation, business trust, estate trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, or instrumentality, public corporation, or any other legal or commercial entity who conducts business in this State and who owns or licenses computerized data that includes personal information.
Definition of Personal Information	Delaware resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to that individual: • Social Security number • Driver's license number or state or federal identification card number • Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account • Passport number • A username or email address, in combination with a password or security question and answer that would permit access to an online account • Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health-care professional, or deoxyribonucleic acid (DNA) profile • Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person • Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes • An individual taxpayer identification number *Exceptions:* Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.
Definition of Breach	An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. *Exception:* Good-faith acquisition of personal information by an employee or agent of any person for the purposes of such person is not a breach of security, provided that the personal information is not used for an unauthorized purpose or subject to further unauthorized disclosure.

Definition of Breach	The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information is not a breach of security to the extent that personal information contained therein is encrypted, unless such unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.
Threshold for Notification	When the following occurs, in order: 1. The covered entity must conduct "in good faith a reasonable and prompt investigation to determine the likelihood that personal information has or will be misused." 2. The investigation must confirm misuse or likely misuse of personal information. *Exceptions:* If the personal information was retrieved in good faith.
Notification of Data Subject	Yes. Any Entity to which the statute applies shall, provide notice of any breach of security following determination of the breach of security to any resident of DE whose personal information was breached or is reasonably believed to have been breached. Notification is not required if the Entity reasonably determines that the breach is unlikely to result in harm to the individuals whose personal information has been breached.
Notification of Government	Yes, to Delaware's attorney general if number of people affected exceeds 500; notice must be provided no later than it is provided to residents of the state.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Third party must give notice if covered entity maintains covered information on behalf of other entity as soon as possible and without delay.

Timing of Notification	Notice must be made without unreasonable delay but not later than 60 days after determination of the breach of security. *Exceptions:* • Shorter time is required under federal law. • A law-enforcement agency determines that the notice will impede a criminal investigation and such law-enforcement agency has made a request of the person that the notice be delayed. Any such delayed notice must be made after such law-enforcement agency determines that notice will not compromise the criminal investigation and so notifies the person of such determination. • When a person otherwise required to provide notice, could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of this State was included in a breach of security, such person must provide the notice to such residents as soon as practicable after the determination that the breach of security included the personal information of such residents, unless such person provides or has provided substitute notice.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Via telephone • Electronically: if the method and content of communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $75,000 • The number of affected entities exceeds 100,000 • Contact information for affected entities is unavailable • Prior efforts to contact affected entities were unsuccessful *Alternate forms of notification:* • Email the affected entity if email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media

Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's "timing requirements" and so long as the entity's notification procedures require the entity to notify individuals and the state's attorney general in the event of an unreasonable breach. *Following agency guidelines?* Yes, so long as the covered entity follows procedures set forth by its primary financial regulator.
Consequences of Non-Compliance	*Government enforcement?* Yes, at the Attorney General's discretion. *Private right of action?* No.
Credit Monitoring Required	Credit Monitoring Required for 12 months if breach included SSN.

District of Columbia

State and Statute	D.C. Off'l Code § 28-3851 et seq.
Covered Entities	Individuals or entities that conduct business in DC and own or license personal information about DC residents in the form of computerized "or other electronic" data. Covered entities "[do] not own" such data.
Definition of Personal Information	Information containing an individual's name and one or more of the following: • Social Security number • Driver's license number or other DC identification number • Credit card, debit card, and/or bank account number • Information necessary to access financial accounts (including but not limited to passwords and PIN numbers) *Exceptions:* Any information about an individual made public by the federal, state, and/or local government.
Definition of Breach	An unauthorized retrieval of "computerized or other electronic data, or any equipment or device storing such data" that "compromises the security, confidentiality, or integrity" of personal information. *Exceptions:* Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party.
Threshold for Notification	When the covered entity discovers any breach of the security of the system. *Exceptions:* If the personal information was retrieved in good faith.
Notification of Data Subject	Yes. Any Entity to which the statute applies, and who discovers a breach of the security system, shall promptly notify any DC resident whose PI was included in the breach.
Notification of Government	—
Notification of Credit Reporting Agencies	Credit Report agency reporting required so long as personal information for more than 1,000 DC residents has been breached. This does not apply to an Entity who is required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act.
Notification by Third Parties	Third party must give notice if covered entity maintains covered information on behalf of other entity as soon as possible and without delay.

Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay. *Exceptions:* If a government agency determines that disclosure will disrupt a criminal investigation, then a covered entity may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Electronically: if the method and content of communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $50,000 • The number of affected entities exceeds 100,000 • Contact information for affected entities is unavailable • Prior efforts to contact affected entities were unsuccessful *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify "major local and, if applicable, national media"
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's "timing requirements" and so long as the entity notifies individuals and the state's attorney general in conjunction with its procedures. *Following agency's guidelines?* Yes, so long as the covered entity follows procedures set forth by its primary financial regulator. If the entity is covered by Title V of the Gramm-Leach-Bliley Act, it shall be deemed to be in compliance.

Consequences of Non-Compliance	*Government enforcement?* Yes, if the DC attorney general is able to successfully petition the Superior Court of the District of Columbia for "temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by" residents of DC as a result of a violation of notification procedures. The Attorney General may penalize covered entities more than $100 for each violation, "the costs of the action," and "reasonable" attorneys' fees. *Private right of action?* Yes, via civil action initiated by affected residents of DC. Residents may "recover actual damages, the costs of the action, and reasonable attorneys' fees."
Credit Monitoring Required	—

Florida

State and Statute	Florida Stat. Ann. § 501.171
Covered Entities	Sole proprietorships, partnerships, corporations, trusts, estates, cooperatives, associations, and other commercial entities that acquire, maintain, store, or use personal information. Governmental entities are also considered covered entities regarding notification of breach for residents of Florida, credit reporting agencies, and other governmental entities.
Definition of Personal Information	Information containing an individual's first initial/name and last name and one or more of the following: • Social Security number • Driver's license number • Passport number • Military identification number • Similar identification number on a government issued document • Credit card, debit card, and/or bank account number • Information necessary to access financial accounts (including but not limited to passwords and PIN numbers) • Information regarding an individual's medical history, medical records, and/or prior diagnoses • Information necessary to access health insurance account information, such as a policy number or subscription identification number • A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account *Exceptions:* Any information about an individual made public by the federal, state, and/or local government.
Definition of Breach	An unauthorized access of data in electronic form containing personal information. *Exceptions:* Information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

Threshold for Notification	Notification Threshold: when the covered entity "reasonably believes" that the personal information of any Florida resident was accessed as a result of the breach. *Exceptions:* If the personal information was retrieved in good faith.
Notification of Data Subject	Yes. Entity must give notice to each individual in Florida whose personal information was, or the Entity reasonably believes to have been, accessed as a result of the breach. Notice to affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the Entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the affected individuals.
Notification of Government	Yes, to the Florida Department of Legal Affairs if the personal information of 500 or more Florida residents is breached. Covered entities must notify the Department of Legal Affairs "no later than 30 days after the determination of the breach or reason to believe a breach occurred." Covered entities may receive a 15-day extension if good cause for delay is provided in writing to the department. In their breach notification, covered entities must state the following information: • The number of Florida residents affected or potentially affected by the breach • The events surrounding the breach at the time notice is provided • An overview of the services that the covered entities offer affected residents • A copy of the breach notification that was sent to affected residents • Contact information for a representative of the covered entity who may be contacted in the event the Department of Legal Affairs requires additional information • If requested by the Department of Legal Affairs, the covered entity must also provide copies of the police report filed for the incident, "policies in place regarding breach incidents," and "steps that have been taken to rectify the breach"
Notification of Credit Reporting Agencies	Credit agency report required so long as personal information for more than 1,000 Florida residents at a single time has been breached.
Notification by Third Parties	Third party must give notice if covered entity maintains covered information on behalf of other entity as soon as possible and without delay.

Timing of Notification	Notifications must be sent as expeditiously as practicable and without unreasonable delay. Covered entities are required to fulfill notification obligations no later than 30 days after the discovery of the breach or the determination that a breach likely occurred. Law enforcement agencies in Florida may authorize delays "for law enforcement purposes" and may issue authorized waivers that preclude covered entities from notification altogether.
Form of Notification	To the Department (AG): Written notice must include a synopsis of the events surrounding the breach at the time notice is provided; the number of individuals in Florida who were or potentially have been affected by the breach; any services related to the breach being offered or scheduled to be offered, without charge, by the Entity to individuals, and instructions as to how to use such services. A copy of the notice required to affected individuals or an explanation of the other actions taken to give notice to affected individuals. The name, address, telephone number, and e-mail address of the employee or agent of the Entity from whom additional information may be obtained about the breach. Upon the Department's request, the Entity must provide the following information to the Department: a police report, incident report, or computer forensics report; a copy of the policies in place regarding breaches; steps that have been taken to rectify the breach. The Entity may provide supplemental information regarding a breach at any time to the Department. To an affected person, the notification of a breach must include the following information: • The "date, estimated date, or date range" of the breach • An overview of the personal information that was breached or believed to have been breached • Contact information for the covered entity • Notice may be provided by the following methods: written notice sent to the mailing address of the individual in the records of the entity; or email notice sent to the individual's e-mail address in the Entity's records The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 • Contact information for affected entities is unavailable • Prior efforts to contact affected entities were unsuccessful

Form of Notification	*Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside
Exemptions or Safe Harbors	No. *Following agency's guidelines?* Yes, so long as the covered entity follows procedures set forth by its primary financial regulator. Once the financial regulator receives notice of the breach, the covered entity must forward "a copy of such notice" to the Department of Legal Affairs in a "timely" fashion.

Consequences of Non-Compliance	Yes, in two ways:
	• Violation of notification procedures "shall be treated as an unfair or deceptive trade practice in any action brought by the Department of Legal Affairs.
	• Covered entities that fail to provide appropriate notice to the Department of Legal Affairs should be subject to a civil penalty of no greater than $500,000. Penalties apply to each breach, not to each individual affected by the breach:
	  • $1,000 penalty for each day "up to the first 30 days following any violation"
	  • $50,000 penalty for each subsequent 30-day period or portion thereof for up to 180 days
	  • If the violation continues for more than 180 days, in a [penalty] amount not to exceed $500,000
	Private right of action?
	No.

Credit Monitoring Required	—

Georgia

State and Statute	Georgia Code § 10-1-910 et seq.
Covered Entities	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, or any state or local agency or subdivision thereof, including any department, bureau, authority, public university or college, academy, commission, or other government entity that maintains computerized data that includes personal information of individuals. "Person" means any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other entity. *Exceptions:* The statute shall not apply to any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.
Definition of Personal Information	"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: • Social Security number • Driver's license number or state identification card number • Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords • Account passwords or personal identification numbers or other access codes • Any of the items above when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised *Exceptions:* Any information about an individual made public or the federal, state, and/or local government records lawfully made public.
Definition of Breach	An unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector. *Exceptions:* If the personal information was retrieved in good faith by an employee or agent for the purposes of the information/data collector.

Threshold for Notification	When the covered entity discovers a breach in the security of the data of any resident of Georgia whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Data Subject	Yes. Any Entity that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach to any resident of GA whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Government	No.
Notification of Credit Reporting Agencies	If personal information for more than 10,000 people has been breached at a single time, reporting credit agencies should be informed.
Notification by Third Parties	—
Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay. *Exceptions:* If a government agency determines that disclosure will disrupt a criminal investigation, then a covered entity may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Via telephone • Electronically: if the method and content of communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $50,000 • The number of affected entities exceeds 100,000 • Contact information for affected entities is unavailable • Prior efforts to contact affected entities were unsuccessful

Form of Notification	*Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notice to major media in urban and rural areas where the affected individuals reside
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's timing requirements and so long as the entity notifies individuals and the state's attorney general in conjunction with its procedures. *Following agency's guidelines?* No.
Consequences of Non-Compliance	*Government enforcement?* Yes, violations may result in civil penalties. *Private right of action?* No.
Credit Monitoring Required	If an entity maintains covered info on behalf of another entity, that entity must notify them within 24 hours of the discovery of a breach if the covered information was, or is reasonably believed to have been, acquired by an unauthorized person.

Guam

State and Statute	Guam 9 GCA § 48.10 et seq.
Covered Entities	An individual or entity that owns or licenses computerized data that includes personal information.
Definition of Personal Information	Information containing an individual's first initial/name and last name and one or more of the following: • Social Security number • Driver's license number or state ID number • Credit card, debit card, and/or bank account number in combination with information necessary to access financial accounts (including but not limited to passwords and PIN numbers) *Exceptions:* Any information about an individual made public or the federal, state, and/or local government records lawfully made public.
Definition of Breach	An unauthorized access and acquisition that compromises the security or confidentiality of the covered information. *Exceptions:* Good-faith acquisitions by employees or agents.
Threshold for Notification	When the covered entity discovers the breach of the security of the system to any resident of Guam whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person, and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of Guam.
Notification of Data Subject	Yes. Third-party reporting required if covered entity maintains covered information on behalf of other entity as soon as possible and without delay.
Notification of Government	No.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	—

Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay. *Exceptions:* If a government agency determines that disclosure will disrupt a criminal investigation, then a covered entity may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Via telephone • Electronically The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $10,000 • The number of affected entities exceeds 5,000 • Contact information or consent for affected entities is unavailable *Alternate forms of notification, any two of the following:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notice to major Guam media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* No. *Following agency's guidelines?* Yes, for financial institutions, so long as the financial institution follows procedures set forth by its primary financial regulator.
Consequences of Non-Compliance	*Government enforcement?* Yes, violations may result in civil penalties not exceeding $150,000 per breach or series of similar breaches discovered in a single investigation. *Private right of action?* No.
Credit Monitoring Required	—

Hawaii

State and Statute	Hawaii Rev. Stat. § 487N-1 et seq.
Covered Entities	Businesses that own or license personal information in any form (whether computerized, paper, or otherwise). The statute covers personal information about Hawaii residents and personal information in general. The statute also applies to any government agency that collects personal information for specific government purposes. A business is defined as a sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit. Also includes financial institutions and entities whose business is records destruction. A government agency is defined as any department, division, board, commission, public corporation, or other agency or instrumentality of the State or of any county.
Definition of Personal Information	Information containing an individual's first initial/name and last name and one or more of the following: • Social Security number • Driver's license number or state ID number • Credit card, debit card, and/or bank account number • Information necessary to access financial accounts (including but not limited to passwords and PIN numbers) *Exceptions:* Any information about an individual made public by the federal, state, and/or local government
Definition of Breach	An unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred. *Exceptions:* Encrypted or redacted information. Good-faith acquisition of personal information by an employee or agent of the Entity for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.
Threshold for Notification	When a covered entity determines that a breach of personal information occurred or is reasonably likely to occur. The breach must also create a risk of harm to the individual whose information is breached. *Exceptions:* If the personal information was retrieved in good faith by an employee or agent for a legitimate purpose.

Notification of Data Subject	Any Entity to which the statute applies shall provide notice to the affected person of a security breach following discovery or notification of the breach.
Notification of Government	Yes, so long as personal information for more than 1,000 people has been breached at a single time. Covered entities must provide notice to the State of Hawaii's Office of Consumer Protection.
Notification of Credit Reporting Agencies	Credit agency reporting required so long as personal information for more than 1,000 people has been breached at a single time.
Notification by Third Parties	Third-party notice required if covered entity maintains covered information on behalf of other entity immediately after breach.
Timing of Notification	Notifications must be sent without unreasonable delay. If a government agency determines that disclosure will disrupt a criminal investigation, then a covered entity may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Via telephone: contact should be made directly with the affected persons • Electronically: if the affected entity's preferred method of communication with the information collector is via electronic means or if the method and content of electronic communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act The notification of a breach must be clear and conspicuous and include the following information: • The incident in general terms • The types of personal information that were breached • How the covered entity has acted to protect the affected person's personal information from further unauthorized access • Contact information for the covered entity • Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $100,000 • The number of affected entities exceeds 200,000 • Contact information for affected entities is unavailable • Prior efforts to contact affected entities were unsuccessful

Form of Notification	*Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media A government agency shall submit a written report to the legislature within 20 days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring.
Exemptions or Safe Harbors	*Following entity's own notification procedures?* No. *Following agency's guidelines?* Yes, for two types of entities: • Financial institutions subject to the text (and any subsequent revisions of) the Federal Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Customer Notice or the National Credit Union Administration's Guidelines for Safeguarding Member Information. • Healthcare plans and providers subject to the privacy standards of the Health Insurance Portability and Accountability Act of 1996.
Consequences of Non-Compliance	*Government enforcement?* Yes, via Hawaii's attorney general or the director of the State of Hawaii's Office of Consumer Protection; covered entities found in violation of notification procedures will be "subject to penalties of not more than $2,500 for each violation. *Private right of action?* Yes, covered entities found in violation of notification procedures will be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. Covered entities may also be held liable for the attorneys' fees of affected parties.
Credit Monitoring Required	—

Idaho

State and Statute	Idaho Code Ann. § 28-51-104 et seq.
Covered Entities	Government agencies at the state, county, and city level; individuals; and commercial entities that conduct business in Idaho and own or have the license to personal information of Idaho residents in the form of computerized data. A commercial entity is defined as a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture and any other legal entity, whether for profit or not-for-profit.
Definition of Personal Information	Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: • Social Security number • Driver's license number or Idaho identification card number • Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account *Exceptions:* The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.
Definition of Breach	An illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons maintained by an agency, individual, or a commercial entity. *Exceptions:* Good-faith acquisition of the personal information by an employee or agent.
Threshold for Notification	When the covered entity conducts, in good faith, a reasonable and prompt investigation that determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur.
Notification of Data Subject	Yes. An Entity to which the statute applies shall give notice as soon as possible to the affected ID resident. *Exceptions:* Notification is not required if after a good-faith, reasonable, and prompt investigation the Entity determines that the personal information has not been and will not be misused.

Notification of Government	Yes, to the Idaho attorney general's office within 24 hours of discovering a breach.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Third-party notice required if covered entity maintains covered information on behalf of other entity immediately after breach.
Timing of Notification	Notifications must be sent in the most expeditious manner possible and without unreasonable delay. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing to the most recent address available in its records • Electronically: if the method and content of electronic communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act • Via telephone The information collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $25,000 • The number of affected entities exceeds 50,000 • Contact information for affected entities is unavailable • Prior efforts to contact affected entities were unsuccessful *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's "timing requirements" and so long as the covered entity notifies individuals in conjunction with its procedures. *Following agency guidelines?* Yes, so long as the covered entity follows procedures set forth by its primary financial regulator.

Consequences of Non-Compliance	*Government enforcement?* Yes, via the primary regulator of a covered entity; primary regulators may bring a civil action to enforce compliance with that section and enjoin that agency from further violations. Covered entities in violation of notification procedures will be subject to a penalty of no more than $25,000 per breach. *Criminal charges against government employees?* Yes, any governmental employee who intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor and, upon conviction thereof, shall 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 right of action?* No.
Credit Monitoring Required	—

Illinois

State and Statute	815 Illinois Comp. Stat. 530/1 et seq.
Covered Entities	Data collectors that own or have the license to personal information of Illinois residents. A data collector may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

Definition of Personal Information	"Personal information" means either of the following:
	• An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted, but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security.
	  • Social Security number
	  • Driver's license number or State identification card number
	  • Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account
	  • Medical information, including 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
	  • Health insurance information, including 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.
	  • Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data
	• Username or email address, in combination with a password or security question and answer that would permit access to an online account, when either the username 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 breach of security.

Definition of Personal Information	*Exceptions:* "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Definition of Breach	An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. *Exceptions:* If the personal information was retrieved in good faith.
Threshold for Notification	When a breach of personal information occurs.
Notification of Data Subject	Yes. Third-party notice required if covered entity maintains covered information on behalf of other entity immediately after breach.
Notification of Government	[Effective January 1, 2020] Any Entity required to disclose a breach of the security system to more than 500 Illinois residents must provide notice to the Attorney General of the breach, including a description of the nature of the breach of security or unauthorized acquisition, the date of the breach, the number of Illinois residents affected by such incident at the time of notification, and any steps the Entity has taken or plans to take relating to the incident. If the date of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date of the breach as soon as possible.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	—
Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.

Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Electronically: if the method and content of electronic communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act The notification of a breach must include, but is not limited to, the following information: • Toll-free phone numbers and addresses for the Federal Trade Commission and consumer reporting agencies • A statement that the affected individual can obtain information from these sources about fraud alerts and security freezes • The notification must not include information concerning the number of Illinois residents affected by the breach The data collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 • Contact information for affected entities is unavailable • Prior efforts to contact affected entities were unsuccessful *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's timing requirements and so long as the covered entity notifies individuals in conjunction with its procedures. *Following agency guidelines?* No.

Consequences of Non-Compliance	*Government enforcement?* Yes, via Illinois's attorney general. The attorney general may seek a number of remedies under the Illinois Consumer Fraud and Deceptive Businesses Act if covered entities violate notification procedures. See 815 Ill. Comp. Stat. 505. Remedies range from civil penalties of up to $50,000 to the cancelation of a covered entity's right to operate its business in Illinois. [Injunctive relief; restitution; and civil penalties]. Covered entities are subject to a civil penalty of up to $50,000 per violation if found in violation of state notification procedures. Additionally, covered entities found in violation of notification procedures against an individual aged 65 or above are subject to civil penalties of up to $10,000 per violation. *Private right of action?* Private individuals may bring suit under the Illinois Consumer Fraud and Deceptive Businesses Act. See 815 Ill. Comp. Stat. 505. Section 10(a) of the Act states that "[a]ny person who suffers actual damage as a result of a violation of this Act committed by another person may bring an action against such person."
Credit Monitoring Required	—

Indiana

State and Statute	Indiana Code § 24-4.9
Covered Entities	Data base owners that own or have the license to personal information in the form of computerized data. Data base owners are defined as individuals who own or license computerized data that includes personal information.

Definition of Personal Information	"Personal information" means:
	• A Social Security number that is not encrypted or redacted
	• An individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:
	  • A driver's license number
	  • A state identification card number
	  • A credit card number
	  • A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account
	
	Exceptions:
	"Personal information" does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

Definition of Breach	Breach: an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.
	
	Exceptions:
	• Good-faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure.
	• Unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key:
	  • Has not been compromised or disclosed; and
	  • Is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.

Threshold for Notification	Notification Threshold: when the personal information of an Indiana resident has been breached and the data base owner 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 an Indiana resident.
Notification of Data Subject	Yes, so long as one of the following occurs: • An unauthorized person has access to or has acquired unencrypted personal information of the Indiana resident. • An unauthorized person has access to or has acquired the "encryption key" required to access personal information of the Indiana resident.
Notification of Government	Yes, to Indiana's Attorney General.
Notification of Credit Reporting Agencies	Credit agency reporting required so long as the personal information of more than 1,000 Indiana residents has been breached.
Notification by Third Parties	Third-party notification required if covered entity maintains covered information on behalf of other entity.
Timing of Notification	Notifications must be sent without unreasonable delay. Delays are reasonable if they meet one or more of the following qualifications: • The delay is necessary to restore the integrity of the computer system. • The delay is necessary to discover the scope of the breach. • Notification is delayed in response to a request from the state attorney general or a law enforcement agency to delay disclosure because disclosure will impede a criminal or civil investigation; or jeopardize national security.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Via mail • Via telephone • Via fax • Via email: if the affected entity's preferred method of communication with the information collector is via email

Form of Notification	The data collector may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 *Alternate forms of notification:* • Conspicuous disclosure of information on the covered entity's website • Notify major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, as long as the "privacy policy" of the covered entity is "at least as stringent as" Indiana and the federal government's notification requirements. *Following agency guidelines?* Yes, so long as the covered entity "maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under" certain federal statutes and guidelines. The covered entity's plan must also require that Indiana residents "be notified of a breach of the security of data without unreasonable delay." The federal statutes and guidelines include: • The U.S.A. Patriot Act P.L. 107-56 • Executive Order 13224 • Driver's Privacy Protection Act 18 U.S.C. 2781 et seq. • Fair Credit Reporting Act 15 U.S.C. 1681 et seq. • Financial Modernization Act of 1999 15 U.S.C. 6801 et seq. • Health Insurance Portability and Accountability Act P.L. 104-191 Financial institutions that comply with the disclosure requirements set by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance Response Programs for Unauthorized Access to Member Information and Member Notice.
Consequences of Non-Compliance	*Government enforcement?* Yes, via Indiana's attorney general; the attorney general may bring action against covered entities that violate the state's notification procedures for deceptive practices. Injunctions, civil penalties of $150,000 or less per deceptive act, and attorneys' fees are among the penalties that can be sought against violators. *Private right of action?* No; expressly states that only the attorney general can act upon violations.
Credit Monitoring Required	—

Iowa

State and Statute	Iowa Code § 715C.1-2
Covered Entities	Any person who owns or licenses personal information in the form of computerized data. Personal information must be used in the course of the person's business, vocation, occupation, or volunteer activities. A person is defined as an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, or instrumentality, public corporation, or any other legal or commercial entity.
Definition of Personal Information	Personal information means information containing an individual's name and one or more of the following: • Social Security number • Driver's license number or other unique identification number created or collected by a government body • Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account • Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account • Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data *Exceptions:* "Personal information" does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.
Definition of Breach	Unauthorized retrieval of computerized data that "compromises the security, confidentiality, or integrity" of personal information. Unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. *Exceptions:* If the personal information was acquired in good faith by employees or agents for a legitimate purpose.
Threshold for Notification	—
Notification of Data Subject	Yes, regardless of residence.

Notification of Government	Yes, to the Attorney General within five business days of breach if more than 500 Iowa residents are affected.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Third-party notice required if covered entity maintains covered information on behalf of other entity immediately after breach.
Timing of Notification	Notifications must be sent in the most expeditious manner possible and without unreasonable delay. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing to the last available address in the covered entity's records • Electronically: if the affected entity's preferred method of communication with the information collector is via electronic means and if the method and content of electronic communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act The notification of a breach must include each of the following: • An overview of the breach • The approximate date of the breach • The types of personal information breached • Contact information for consumer reporting agencies • Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the [state] attorney general The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 350,000 • Contact information for affected entities is unavailable *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media

Exemptions or Safe Harbors	*Following entity's own notification procedures?* No. *Following agency guidelines?* Yes, if the covered entity's notification procedures meet any of the following: A person who complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator. A person who complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section. The covered entity is subject to and complies with regulations promulgated pursuant to Title V of the Gramm Leach Bliley Act. The covered entity is subject to and complies with regulations promulgated pursuant to Title II of the Health Insurance Portability and Accountability Act and Title XIII of the Health Information Technology for Economic and Clinical Health Act.
Consequences of Non-Compliance	*Government enforcement?* Yes, via Iowa's attorney general. The attorney general can seek penalties under consumer fraud law in Iowa and can also require the violating party to pay damages to the attorney general on behalf of the injured party or parties. *Private right of action?* No, although the attorney general may seek damages on behalf of a private individual.
Credit Monitoring Required	—

Kansas

State and Statute	Kansas Stat. § 50-7a01 et seq.
Covered Entities	A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information. 'Person' means any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency or other entity.
Definition of Personal Information	Personal information means a Kansas citizen's first name or first initial and last name linked to any one or more of the following data elements that relate to the citizen, when the data elements are neither encrypted nor redacted: • Social Security number • Driver's license number or state identification card number • Financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a citizen's financial account *Exceptions:* The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Definition of Breach	An unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer. *Exceptions:* Good faith acquisition of personal information by an employee or agent of an individual or commercial entity for the purposes of such entity, provided there is no further unauthorized disclosure.
Threshold for Notification	When the covered entity becomes aware of any breach of the security of the system, conducts in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused.
Notification of Data Subject	Yes.
Notification of Government	No.
Notification of Credit Reporting Agencies	Credit agency reporting required so long as notifications of a breach must be sent to more than 1,000 residents at once.

Notification by Third Parties	Third-party notice required if covered entity maintains covered information on behalf of other entity if the information was or is reasonably believed to have been accessed by an unauthorized person.
Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • In writing • Electronically: if the affected entity's preferred method of communication with the information collector is via electronic means and if the method and content of electronic communication meets definitions set forth in the Electronic Signatures in Global and National Commerce Act The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $100,000 • The number of affected entities exceeds 5,000 • Contact information for affected entities is unavailable *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's timing requirements and so long as the entity notifies individuals in conjunction with its procedures. *Following agency guidelines?* Yes, if the covered entity maintains notification procedures subject to requirements of its primary federal regulator and those requirements are deemed to be in compliance with Kansas's notification requirements.

Consequences of Non-Compliance	*Government enforcement?* Yes, via Kansas's attorney general. The attorney general may seek appropriate relief for violations of notification procedures. However, if violations regard an insurance company that legally conducts business in Kansas, Kansas's insurance commissioner has the sole authority to enforce the provisions of Kansas's notification procedures. *Private right of action?* No.
Credit Monitoring Required	—

Kentucky

State and Statute	Kentucky Rev. Stat. Ann. § 365.732.
Covered Entities	Any person or business entity that conducts business in Kentucky.
Definition of Personal Information	"Personally identifiable information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or data element is not redacted: • Social Security number • Driver's license number • Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account
Definition of Breach	An unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of Kentucky. *Exceptions:* Good faith acquisition of personally identifiable information by an employee or agent of a covered entity only for the purposes of such entity and not subject to further unauthorized disclosure.
Threshold for Notification	When the covered entity discloses any breach of the security of the system, following discovery or notification of the breach in the security of the data.
Notification of Data Subject	Yes.
Notification of Government	—
Notification of Credit Reporting Agencies	Credit agency reporting so long as notifications of a breach must be sent to more than 1,000 residents at once.
Notification by Third Parties	Third-party notice required if covered entity maintains covered information on behalf of other entity if the information was or is reasonably believed to have been accessed by an unauthorized person.
Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.

Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written notice • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 • Contact information for affected entities is unavailable *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's timing requirements and so long as the entity notifies individuals in conjunction with its procedures. *Following agency guidelines?* No. The provisions for covered entities and non-affiliated third party requirements shall not apply to entities covered by Title V of the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act.
Consequences of Non-Compliance	*Government enforcement?* The Kentucky Board of Education may promulgate administrative regulations in accordance with KRS Chapter 13A as necessary to carry out the requirements of this section. *Private right of action?* Statute is silent on private right of action. But *see In re Target Corp. Data Sec. Breach Litigation*, MDL No. 14-2522, 2014 WL 7192478 (Dec. 18, 2014) (Declining to dismiss a claim because Kentucky's data breach statute lacks an explicit private right of action).
Credit Monitoring Required	—

Louisiana

State and Statute	Louisiana Stat. Ann. §51:3071-7 (2014)
Covered Entities	Any person that conducts business in Louisiana or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information. "Person" means any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity.
Definition of Personal Information	"Personal information" means the first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: • Social Security number • Driver's license number or state identification card number • Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account • Passport number • Biometric data: data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voiceprint, 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 *Exceptions:* The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Definition of Breach	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. *Exceptions:* If the personal information was retrieved in good faith by an employee or an agent and was not subject to further disclosure.
Threshold for Notification	When the covered entity discovers a breach. *Exception:* No notification is necessary if, after a reasonable investigation, the entity determines that there is no reasonable likelihood of harm. The covered entity must document determination in writing, retain the documentation for five years, and provide a copy to the Attorney General upon request.

Notification of Data Subject	Yes, any person that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. And, any agency or person that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system.
Notification of Government	Yes, if notice to Louisiana residents is required, the covered entity must also provide written notice to the Consumer Protection Section of the Attorney General's office. Notice must be received within 10 days of distribution of notice to Louisiana residents and must include the names of those affected residents.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	—
Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay, but in any event no later than 60 days after the discovery of the breach. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written notice • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $100,000 • The number of affected entities exceeds 100,000 • Contact information for affected entities is unavailable

Form of Notification	*Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the covered entity's own notification procedures are consistent with the statute's timing requirements and so long as the entity notifies individuals in conjunction with its procedures. *Following agency guidelines?* No.
Consequences of Non-Compliance	*Government enforcement?* Yes, a violation of the statute also constitutes an unfair act or practice under LA law. Failure to provide timely notification to the Consumer Protection Section of the Attorney General's Office may result in a fine of up to $5,000 per violation. Notice to the state Attorney General shall be timely if received within 10 days of distribution of notice to LA citizens. Each day the Attorney General does not receive notice is a separate violation. *Private right of action?* Yes, the statute provides a private right of action to recover actual damages resulting from the failure to disclose breach in a timely manner.
Credit Monitoring Required	—

Maine

State and Statute	Maine Rev. Stat. Ann. tit. 10, § 1346-49
Covered Entities	Information brokers, defined as: a person who, for monetary purposes, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating personal information to non-affiliated third parties. Persons, includes: an individual or other legal entity, including higher education institutions and government agencies. *Exceptions:* Does not include government agencies whose records are maintained for traffic safety, law enforcement, or licensing purposes.
Definition of Personal Information	An individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: • Social Security number • Driver's license number or state identification card number • Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords • Account passwords or personal identification numbers or other access codes • Any of the data elements contained above when not in connection with the individual's first name, or first initial, and last name, if the information, if compromised, would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised *Exceptions:* "Personal information" does not include information from third-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.
Definition of Breach	An unauthorized acquisition, release, or use of an individual's computerized data that includes personal information that compromises the security, confidentiality, or integrity of personal information of the individual maintained by a person. *Exceptions:* If the personal information was retrieved in good faith by an employee or agent.

Threshold for Notification	When the covered entity discovers a breach and determines that personal information has been or will likely be misused. *Exception:* No notification is necessary if, after a reasonable investigation, the entity determines that there is no reasonable likelihood of harm.
Notification of Data Subject	Yes, an information broker shall give notice of a breach of the security of the system following discovery or notification of the security breach to a ME resident whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. Any other person shall give notice of a breach of the security of the system following discovery or notification of the security breach to a ME resident if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.
Notification of Government	Yes, the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney General.
Notification of Credit Reporting Agencies	Notice to credit reporting agencies so long as notifications of a breach is sent to more than 1,000 residents at once.
Notification by Third Parties	Third party required to give notice if covered entity maintains covered information on behalf of other entity immediately following the discovery of the breach if the information was or is reasonably believed to have been accessed by an unauthorized person.
Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written notice • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act

Form of Notification	The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $5,000 • The number of affected entities exceeds 1,000 • Contact information for affected entities is unavailable *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the notification procedures are consistent with the statute's timing requirements and so long as the guidelines provide for notification procedures at least as protective as the notification requirements under this statute. *Following agency guidelines?* No.
Consequences of Non-Compliance	*Government enforcement?* Yes, other than certain state agencies, a covered entity is subject to one or more of the following: • Civil fines of not more than $500 per violation, up to a maximum of $2,500 for each day the violation exists • Equitable relief • Injunction from future violations *Private right of action?* No.
Credit Monitoring Required	—

Maryland

State and Statute	Maryland Code Ann., Commercial Law § 14-3501 et seq.
Covered Entities	A business that owns or licenses computerized data that includes personal information of an individual residing in the State, or a business that maintains computerized data that includes personal information of an individual residing in the State that the business does not own or license. Business means a sole proprietorship, partnership, corporation, association or any other business entity, whether or not organized to operate at a profit.
Definition of Personal Information	"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: • A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government • A driver's license number or state identification card number • An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account • Health information, including information about an individual's mental health. "Health information" means any information created by an entity covered by HIPAA regarding an individual's medical history, medical condition, or medical treatment or diagnosis • A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information. • Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account • A username or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account *Exceptions:* "Personal information" does not include: • Publicly available information that was lawfully made public by local, state, or federal government • Information the individual has consented to have released • Information disseminated or listed in accordance with HIPAA

Definition of Breach	An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information managed by a business. *Exception:* If the personal information was retrieved in good faith by an employee or agent for purposes of the business and not subject to further unauthorized disclosure.
Threshold for Notification	When the covered entity discovers a breach and determines that personal information has been or will likely be misused. *Exception:* No notification is necessary if after a reasonable investigation the entity determines that there is no reasonable likelihood of harm. The covered entity must document determination in writing, and retain the documentation for 3 years.
Notification of Data Subject	Yes, if the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the owner or licensee of the computerized data shall notify the individual of the breach.
Notification of Government	Yes, the covered entity must report to Maryland Attorney General before providing consumer notice.
Notification of Credit Reporting Agencies	Notice to credit reporting agencies so long as notifications of a breach must be sent to more than 1,000 residents at once.
Notification by Third Parties	Third party notice required if covered entity maintains covered information on behalf of other entity as soon as practicable, but in any case no later than 45 days after discovery of the breach.
Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay, but if any event no later than 45 days after the covered entity concludes their investigation. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation any longer, but by no later than 30 days after concluding the investigation. The notification can also be delayed to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.

Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written notice • Telephonic notice • Electronic notice, if the individual has expressly consented to receive electronic notice; or the business conducts its business primarily through Internet account transactions or the Internet The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $100,000 • The number of affected entities exceeds 175,000 • Contact information for affected entities is unavailable The notification must include: • A description of the information breached • Contact information for the business making the notification • Toll-free numbers and addresses for major credit reporting agencies • Toll-free numbers, addresses, and website addresses for the FTC and the AG's office • A statement that the individual can obtain information from these sources for next steps *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media

Exemptions or Safe Harbors	*Following entity's own notification procedures?*
	No.
	
	Following agency guidelines?
	No.
	
	The following are deemed to be in compliance:
	• Businesses that comply with requirements of it's own primary regulator
	• Businesses in compliance with the:
	  • Gramm-Leach-Bliley Act
	  • Fair and Accurate Credit Transactions Act
	  • Interagency Guidelines Establishing Information Security Standards
	  • Interagency Guidance on Response Programs for Unauthorized Access to Customer Information & Notice

Consequences of Non-Compliance	*Government enforcement?* Yes, civil fines of not more than $500 per violation, up to a maximum of $2,500 for each day the violation exists; equitable relief; enjoinment from future violations. *Private right of action?* No.
Credit Monitoring Required	—

Massachusetts

State and Statute	Massachusetts Gen. Laws Ann. ch. 93H, § 1 et seq.
Covered Entities	A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth. "Agency", any agency, executive office, department, board, commission, bureau, division, or authority of the commonwealth, or any of its branches, or of any political subdivision thereof. "Person", a natural person, corporation, association, partnership, or other legal entity.
Definition of Personal Information	"Personal information" is a resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: • Social Security number • Driver's license number or state-issued identification card number • Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account *Exceptions:* "Personal information" does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.
Definition of Breach	An unauthorized acquisition or unauthorized use of unencrypted data or, 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. *Exception:* A good faith acquisition by an employee or agent for lawful purposes.
Threshold for Notification	When the covered entity (1) knows or has reason to know of a breach of security, or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.
Notification of Data Subject	Yes, the notice to be provided to the resident shall include, but shall not be limited to: • The resident's right to obtain a police report • How a resident may request a security freeze and the necessary information to be provided when requesting the security freeze • That there shall be no charge for a security freeze

Notification of Data Subject	• Mitigation services to be provided pursuant to this chapter; provided, however, that said notice shall not include the nature of the breach of security or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach of security or unauthorized access or use. The person or agency that experienced the breach of security shall provide a sample copy of the notice it sent to consumers to the Attorney General and the Office of Consumer Affairs and Business Regulation (OCABR). A notice provided pursuant to this section shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information.
Notification of Government	Yes, the attorney general and the Director of OCABR as soon as practicable and without unreasonable delay.
Notification of Credit Reporting Agencies	Notice to credit reporting agencies at the discretion of the OCABR.
Notification by Third Parties	Notice from third party required if covered entity maintains covered information on behalf of other entity as soon as practicable and without unreasonable delay following the breach if the information was or is reasonably believed to have been accessed by an unauthorized person.
Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay on a rolling basis. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written notice • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act • Telephonic notice if the notice is not given in whole or in part by recording, and the recipient has expressly agreed to receive notice by phone. If the recipient has not consented, telephonic notice can be provided if the entity also provides follow-up notice if the recipient does not answer the phone or call back within three business days.

Form of Notification	The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 The notification must include: • A description of the breach • A description of the type of information breached • Any steps the person or agency plans to take relating to the breach • A telephone number where the recipient can obtain assistance or additional information • A reminder of the recipient's need to stay vigilant to avoid identity fraud *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes. *Following agency guidelines?* No.
Consequences of Non-Compliance	*Government enforcement?* Yes, The Attorney General may bring an action in the commonwealth's name under Massachusetts' consumer protection law to remedy violations and for other relief that may be appropriate. The Attorney General may seek: • Injunctive relief • If the covered entity knew or should have known it was in violation of the statute: a $5,000 penalty for each violation and reasonable costs and attorneys' fees *Private right of action?* No.
Credit Monitoring Required	Credit Monitoring Required for 18 months if a breach involves a resident's SSN at no cost.

Michigan

State and Statute	Michigan Comp. Laws Ann. §445.63, 445.72
Covered Entities	All persons or agencies owning or licensing data stored in databases. "Person" means an individual, partnership, corporation, limited liability company, association, or other legal entity. "Agency" means a department, board, commission, office, agency, authority, or other unit of state government of this state. The term includes an institution of higher education of this state. The term does not include a circuit, probate, district, or municipal court.
Definition of Personal Information	"Personal information" means the first name or first initial and last name linked to one or more of the following data elements of a resident of Michigan: • Social Security number • Driver license number or state personal identification card number • Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts *Exceptions:* ''Personal information'' does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.
Definition of Breach	An unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals. *Exceptions:* These terms do not include unauthorized access to data by an employee or other individual if the access meets all of the following: • The employee or other individual acted in good faith in accessing the data. • The access was related to the activities of the agency or person. • The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.
Threshold for Notification	Notification Threshold: when the covered entity discovers or notices a breach that resulted in the unauthorized access to unencrypted personal information, or encrypted information with the necessary access key. *Exceptions:* Notice is not required if it is determined that the breach has not or is not likely to cause substantial injury or identity theft.

Notification of Data Subject	Yes, the notice must be written or communicated in a clear and conspicuous manner and include all of the following: • Description of the security breach in general terms • Description of the type of personal information breached • General description of what the covered entity providing the notice has done to protect the data from further security breaches, if applicable • Telephone number where a notice recipient may obtain assistance or additional information • Reminder to affected persons of the need to remain vigilant for fraud and identity theft
Notification of Government	No.
Notification of Credit Reporting Agencies	Credit agency report required, unless the person or agency is required to provide notice of a security breach to 1,000 or fewer residents of this state or the person or agency is subject to the Gramm-Leach-Bliley Act.
Notification by Third Parties	Notice from a third party required unless the breach has not and is not likely to cause substantial loss or injury to one or more Michigan residents.
Timing of Notification	Notifications must be sent in the most expeditious time possible and without unreasonable delay. If the government agency determines that disclosure will disrupt a criminal investigation, then an information collector may delay notification until disclosure will not disrupt the investigation. The notification can also be delayed to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written notice • Electronic notice, if the recipient has expressly consented to receive electronic notice and the person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person or agency reasonably believes that it has the recipient's current electronic mail address

Form of Notification	The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 • Contact information for affected entities is unavailable The notification must include: • Informing the owner or licensor of the breach • The date or approximate date of the breach • A description of the breach • Any steps the person or agency plans to take relating to the breach • The consumer's right to obtain a police report • How a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze • Any fees required to be paid to any of the consumer reporting agencies *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, if the entity is a financial institution with notification procedures in place and subject to examination by an appropriate regulator. *Following agency guidelines?* No. Notice may be provided pursuant to an agreement between the person or agency and another person or agency, if it does not conflict with any provision of this section. Entities subject to and in compliance with HIPAA.
Consequences of Non-Compliance	*Government enforcement?* Yes, civil fine not more than $250 for each violation and up to $750,000 total. *Private right of action?* No, the general statute does not include a private right of action, but explicitly notes that it does not eliminate other remedies available by law.
Credit Monitoring Required	

Minnesota

State and Statute	Minnesota Stat. § 325E.61, 325E.64 Minnesota Stat. 325E.64
Covered Entities	Any person or business that conducts business in Minnesota, and that owns or licenses data that includes personal information. *Exception:* Does not apply to financial institutions.
Definition of Personal Information	An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired: • Social Security number • Driver's license number or Minnesota identification card number • Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account *Exceptions:* "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Definition of Breach	An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. *Exceptions:* If the personal information was retrieved in good faith by an employee or agent for purposes of the person.
Threshold for Notification	When the covered entity discovers the breach in the security of the data to any resident of Minnesota whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Data Subject	Yes, any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification of Government	—
Notification of Credit Reporting Agencies	Notice to credit reporting agencies must be given within 48 hours so long as notifications of a breach must be sent to more than 500 residents at once.
Notification by Third Parties	Third-party notice required immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Timing of Notification	The disclosure must be made in the most expeditious time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written notice • Electronic notice, if the entity's primary communication with the affected individual was electronic, or if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying entities exceeds $250,000 • The number of affected entities exceeds 500,000 • Contact information for affected entities is unavailable *Alternate forms of notification:* • Email the affected entity if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, so long as the notification procedures are consistent with the statute's timing requirements and so long as the guidelines provide for notification procedures at least as protective as the notification requirements under this statute. *Following agency guidelines?* No.

Consequences of Non-Compliance	*Government enforcement?* Yes, by the Attorney General who may seek either or both: injunctive relief and/or a civil penalty not to exceed $25,000. *Private right of action?* No. *See In re Target Corp. Data Sec. Breach Litigation*, 66 F.Supp.3d 1154 (D.Minn. 2014).
Credit Monitoring Required	—

Mississippi

State and Statute	Mississippi Code Ann. § 75-24-29
Covered Entities	Any person conducting business in the state and who, in the ordinary course of the person's business functions, owns, licenses, or maintains personal information of any resident of this state. Person is defined as: natural persons, corporations, trusts, partnerships, incorporated and unincorporated associations, and any other legal entity.
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following: • Social Security Number • Driver's License Number • Account, credit card, or debit card number, along with any required security code, access code or password needed to access the individual's financial account.
Definition of Breach	An unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information of any resident of this state 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. This does not include good-faith acquisitions of personally, identifiable information by employees or agents of the information holder.
Threshold for Notification	Those that own or license personal information shall give notice of any breach of security to all affected individuals. Notification shall not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals. Those that maintain personal information shall notify the owner or licensee of the information of any breach of the security as soon as practicable following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.
Notification of Data Subject	Yes, to "affected individuals", i.e. any Mississippi resident whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security.
Notification of Government	No.

Notification of Credit Reporting Agencies	—
Notification by Third Parties	—
Timing of Notification	The disclosure by the owner or licensee shall be made without unreasonable delay, subject to law enforcement requests for delay and the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system.
Form of Notification	Written, telephonic or electronic (if electronic is usual means of communication and notice is consistent with 15 U.S.C. § 7001). Or substitute notice, if the cost of notification exceeds $5,000, the number of affected individuals is greater than 5,000, or the business has insufficient information for the other forms of notice. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to statewide media
Exemptions or Safe Harbors	Following entity's own notification procedures if those procedures comply with the timing requirements of the statute.
Consequences of Non-Compliance	*Government enforcement?* Enforcement is by the Attorney General as an unfair trade practice. The insurance statute authorizes the Commissioner of Insurance to examine and investigate any licensee to determine whether a violation of the statute has occurred and may take any necessary or appropriate action to enforce the provisions. *Private right of action?* No.
Credit Monitoring Required	—

Missouri

State and Statute	Missouri Ann. Stat. § 407.1500
Covered Entities	Any person that owns, licenses, or maintains personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri. Person is defined as any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity. *Exceptions:* • A person that complies with its own notice procedures that are otherwise consistent with the timing requirements of this law. • A person that is regulated by state or federal law and complies with procedures for a breach of the security of the system pursuant to rules established by its primary or functional state or federal regulator. • Financial institutions that are in compliance with applicable federal privacy and breach notification procedures.
Definition of Personal Information	Personal information means an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable: • Social Security number • Driver's license number or other unique identification number created or collected by a government body • Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account • Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account • Medical information • Health insurance information *Exception:* Information that is lawfully obtained from publicly available sources.

Definition of Breach	An unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. This does not include good-faith acquisitions of personally identifiable information by employees or agents of the information holder.
Threshold for Notification	The owner or licensee shall notify upon discovery or notification of the security breach. Any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach The notice required by this section may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing.
Notification of Data Subject	Yes, the notice shall, at a minimum, include a description of the following: • The incident in general terms • The type of personal information that was obtained as a result of the breach of security • A telephone number that the affected consumer may call for further information and assistance, if one exists • Contact information for consumer reporting agencies • Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports An individual or legal, commercial, or governmental entity that maintains or possesses records or data, which contains personal information that it does not own or license, must notify the information's owner or licensee immediately following a discovery of any breach of security, consistent with the legitimate needs of law enforcement. If, after an appropriate investigation by the third-party custodian or after consultation with the relevant federal, state, or local law enforcement agencies, the custodian 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. A written record of a determination not to provide notice to potentially affected persons must be maintained for five years.
Notification of Government	Yes. The Attorney General must be notified if notice is provided to more than 1,000 consumers at one time pursuant to this law.

Notification of Credit Reporting Agencies	Credit agency notice required if notice is provided to more than 1,000 consumers at one time pursuant to this law. Notice must be given to consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Notification by Third Parties	—
Timing of Notification	Notice shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in this section; and consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.
Form of Notification	Written, telephonic, or electronic (if electronic, consistent with 15 U.S.C. § 7001). Or substitute notice, if the cost of notification exceeds $100,000, the number of affected individuals is greater than 150,000, or the business has insufficient information for the other forms of notice. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to statewide media
Exemptions or Safe Harbors	Entities that are regulated by state or federal law and follow the notification procedures mandated therein.
Consequences of Non-Compliance	*Government enforcement?* The Attorney General has exclusive authority to bring an action for damages for a willful and knowing violation of this section for up to $150,000 per breach, or series of breaches of a similar nature and discovered at the same time. *Private right of action?* No.
Credit Monitoring Required	—

Montana

State and Statute	Montana Code Ann. § 30-14-1704
Covered Entities	Any business or person that conducts business in the state and owns or licenses computerized data that includes personal information of residents. "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records. Person is not defined. *Exception:* Industries regulated under Title 33.
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following: • Social Security Number • Driver's License Number • Account, credit card, or debit card number, along with any required access code needed to access the financial account • Medical record information as defined in 33–19–104 • Taxpayer identification number • Identity protection personal identification number issued by the United States internal revenue service *Exception:* Information that is lawfully obtained from publicly available sources including government records.
Definition of Breach	An unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information and causes or is reasonably believed to cause loss or injury to a Montana resident. This does not include good-faith acquisitions of personally identifiable information by employees or agents of the information holder.
Threshold for Notification	Following discovery or notification of the security breach.

Notification of Data Subject	Yes, any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
Notification of Government	Yes, any person or business that is required to issue a notification pursuant to this section shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the attorney general's consumer protection office, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification. If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individual.
Notification of Credit Reporting Agencies	Credit reporting agencies shall be put on notice without unreasonable delay if the covered entity suggests, indicates, or implies to the individual that the individual may obtain a copy of the file from a consumer credit reporting agency.
Notification by Third Parties	Third-party notice required if the covered entity must notify the information's owner or licensee of any breach of the security of the data system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.
Timing of Notification	Without unreasonable delay. Consistent with the legitimate needs of law enforcement.

Form of Notification	Written, telephonic, or electronic (if electronic, consistent with 15 U.S.C. § 7001). Or substitute notice, if the cost of notification exceeds $250,000, the number of affected individuals is greater than 500,000, or the business has insufficient information for the other forms of notice. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to statewide media
Exemptions or Safe Harbors	Following entity's own notification procedures, if they do not unreasonably delay notification.
Consequences of Non-Compliance	*Government enforcement?* The Attorney General may bring an action for injunctive relief or penalties set out in Montana's Consumer Protection Act, including a civil fine of up to $10,000 for each violation. *Private right of action?* No.
Credit Monitoring Required	—

Nebraska

State and Statute	Nebraska Rev. Stat. Ann. § 87-801
Covered Entities	An individual or commercial entity, defined as any legal entity, whether for-profit or non-profit that conducts business in Nebraska and owns or licenses computerized data that includes personal information about a Nebraska resident. Duties cannot be waived.
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following: • Social Security Number • Driver's License Number or state identification card number • Account, credit card, or debit card number, along with any required security code, access code or password needed to access the financial account • Unique electronic ID or routing code, along with any required security code, access code or password • Unique biometric data, such as fingerprints, voiceprints, and retina or iris images • A username or email address in combination with a password or security question and answer that would permit access to an online account *Exception:* Information that is lawfully obtained from publicly available sources.
Definition of Breach	An unauthorized acquisition of unencrypted data that compromises the security, confidentiality, or integrity of personal information.
Threshold for Notification	If, after a good-faith investigation, it is determined that unauthorized use of personal information has occurred or is reasonably likely to occur. An individual or commercial entity that maintains computerized data that includes personal information on behalf of the owner or licensor must notify and cooperate with such owner or licensee when it becomes aware that the unauthorized use of personal information has occurred or is reasonably likely to occur.
Notification of Data Subject	Yes, any entity to which the statute applies shall, when it becomes aware of a breach of the security of the system and determines that the use of information about a NE resident for an unauthorized purpose has occurred or is reasonably likely to occur, give notice to the affected NE resident. If an 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 breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification of Government	Yes, to the Attorney General.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	—
Timing of Notification	As soon as possible and without unreasonable delay consistent with the legitimate needs of law enforcement and with any measures to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
Form of Notification	Written, telephonic, or electronic (if electronic, consistent with 15 U.S.C. § 7001). Or substitute notice, if the cost of notification exceeds $75,000, the number of affected individuals is greater than 100,000, or the entity has insufficient information for the other forms of notice. Substitute notice must consist of: • Email to those for whom it has email addresses • Paid advertisement in a local newspaper • Conspicuous posting on business's website • Notification to statewide media
Exemptions or Safe Harbors	Following entity's own notification procedures if consistent with this timing requirements of this law. Entities that are regulated by state or federal law and follow the notification procedures mandated therein.
Consequences of Non-Compliance	*Government enforcement?* Enforcement by the Attorney General who may both issue subpoenas and seek and recover direct economic damages for each NE resident injured by a statutory violation. *Private right of action?* No.
Credit Monitoring Required	—

Nevada

State and Statute	Nevada Rev. Stat. Ann. § 603A.220
Covered Entities	Data collectors, defined as any governmental agency, institution of higher education, financial institution, any business entity, or association that owns, licenses, or maintains computerized data that includes personal information. Duties cannot be waived.
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following: • Social Security Number • Driver's License Number • Account, credit card, or debit card number, along with any required access code needed to access the financial account • A medical identification number or a health insurance identification number • A username, 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 *Exception:* This does not include the last four digits of a social security number, the last four digits on any ID card, or information made lawfully publicly available.
Definition of Breach	An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. This does not include good-faith acquisitions of personally, identifiable information by employees or agents of the information holder.
Threshold for Notification	Following discovery or notification of the security breach.
Notification of Data Subject	Yes, any entity to which the statute applies shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of NV whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person. If a Nevada entity maintains computerized data that includes personal information that the entity does not own, it must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Government	—

Notification of Credit Reporting Agencies	Credit agency reporting required if more than 1,000 persons to be notified.
Notification by Third Parties	—
Timing of Notification	In the most expeditious time possible and without unreasonable delay. Consistent with the legitimate needs of law enforcement or any measures to determine the scope of the breach and restore the reasonable integrity of the system data.
Form of Notification	Written or electronic (if electronic, consistent with 15 U.S.C. § 7001). Or substitute notice, if the cost of notification exceeds $250,000, the number of affected individuals is greater than 500,000, or the business has insufficient information for the other forms of notice. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to statewide media
Exemptions or Safe Harbors	Following entity's own notification procedures. Entities subject to the privacy provisions of the Gramm-Leach-Bliley Act.
Consequences of Non-Compliance	*Government enforcement?* The Attorney General may bring an action for a temporary or permanent injunction to stop any violations. *Private right of action?* Yes, a covered entity that provides the requisite notice may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the entity.
Credit Monitoring Required	—

New Hampshire

State and Statute	New Hampshire Rev. Stat. Ann. § 359-C:19, 359-C:20, 359-C:21 New Hampshire Stat. Ann. § 359-C:20 New Hampshire Stat. Ann. § 359-C:21
Covered Entities	All persons doing business in the state. Person is defined as individuals, business and other legal entities, government entities, and political subdivisions. Duties cannot be waived.
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following: • Social Security number • Driver's license number • Account, credit card, or debit card number, along with any required access code needed to access the financial account *Exception:* Information that is lawfully obtained from publicly available sources.
Definition of Breach	An unauthorized acquisition of data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. This does not include the good-faith acquisition of personal information by an employee or agent of a person.
Threshold for Notification	A determination that misuse of personal information has occurred or is reasonably likely to occur. This determination must be promptly made when a person becomes aware of a security breach.
Notification of Data Subject	Yes, any entity to which the statute applies, when it becomes aware of a security breach and determines that misuse of PI has occurred or is reasonably likely to occur, or if a determination cannot be made, shall notify the affected individuals. Notification is not required if it is determined that misuse of the PI has not occurred and is not reasonably likely to occur. The notice must include: • A general description of the security breach • The approximate date of the breach • The telephonic contact information of the covered entity reporting the breach • A list of the types of personal information that were or are reasonably believed to have been the subject of the breach

Notification of Data Subject	If an entity maintains computerized data that includes PI that the entity does not own, the entity shall notify and cooperate with the owner or licensee of the PI of any breach of the security of the data immediately following discovery if the PI was acquired by an unauthorized person. Cooperation includes sharing with the owner or licensee information relevant to the breach, except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets.
Notification of Government	Yes, to the regulator that has primary regulatory authority over the person. All other persons shall notify the New Hampshire Attorney General's office.
Notification of Credit Reporting Agencies	Credit agency reporting required if more than 1,000 persons to be notified.
Notification by Third Parties	—
Timing of Notification	As quickly as possible after the determination is made, consistent with the legitimate needs of law enforcement.
Form of Notification	Written, telephonic, or electronic (if electronic, consistent with 15 U.S.C. § 7001). Or substitute notice, if the cost of notification exceeds $5,000, the number of affected individuals is greater than 1,000, or the business has insufficient information for the other forms of notice. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to statewide media
Exemptions or Safe Harbors	Following entity's own notification procedures. Financial institutions subject to Gramm-Leach-Bliley Act.
Consequences of Non-Compliance	*Government enforcement?* Through the Attorney General who may bring an action in the name of the state to: restrain the violation by temporary or permanent injunction and obtain up to $10,000 in civil penalties for each violation. *Private right of action?* Yes, any person injured by any violation may bring a civil action for damages or equitable relief plus attorneys' fees. If conduct was willful or knowing, damages are automatically doubled and treble damages are available under the discretion of the judge.
Credit Monitoring Required	—

New Jersey

State and Statute	New Jersey Stat. Ann. § 56:8-161, 56:8-163
Covered Entities	Any business or public entity. Business is defined as any entity, however organized, both for-profit and not-for-profit, including financial institutions. Public entity is defined as the state, and any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State.
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following: • Social Security number • Driver's license number • Account, credit card, or debit card number, along with any required access code needed to access the financial account 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. *Exception:* Information that is lawfully obtained from publicly available sources.
Definition of Breach	An unauthorized access to electronic files, media, or data containing personal information that compromises the security, confidentiality, or integrity of personal information. This does not include the good-faith acquisition of personal information by an employee or agent of a business.
Threshold for Notification	Following discovery or notification of breach to resident whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. But not if misuse of the information is not reasonably possible.
Notification of Data Subject	Yes, covered entities shall disclose any breach of security of computerized records following discovery or notification of the breach to any customer who is a resident of NJ whose PI was, or is reasonably believed to have been, accessed by an unauthorized person. An entity that compiles or maintains computerized records that include PI on behalf of another covered entity shall notify that entity of any breach of security of the computerized records immediately following discovery, if the PI was, or is reasonably believed to have been, accessed by an unauthorized person.
Notification of Government	Yes, to the Division of State Police in the Department of Law and Public in advance of the disclosure to the affected persons.

Notification of Credit Reporting Agencies	Credit agency reporting required if more than 1,000 persons to be notified.
Notification by Third Parties	—
Timing of Notification	In the most expeditious time possible and without unreasonable delay consistent with the legitimate needs of law enforcement.
Form of Notification	Written or electronic (if electronic, consistent with 15 U.S.C. § 7001). Or substitute notice, if the cost of notification exceeds $250,000, the number of affected individuals is greater than 500,000, or the business has insufficient information for the other forms of notice. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to statewide media
Exemptions or Safe Harbors	Following entity's own notification procedures.
Consequences of Non-Compliance	*Government enforcement?* The attorney general has enforcement authority and may seek remedies including: • Injunctive relief • Civil penalties of not more than $10,000 for the first offense and not more than $20,000 for each later offense • Costs A municipal or county office of consumer affairs also has enforcement authority. *Private right of action?* Perhaps, the statute states that any willful, knowing, or reckless violation of the data breach notification requirement is an unlawful practice and a violation of Title 56, Chapter 8 of the New Jersey Statutes. In addition to appropriate legal or equitable relief, a court may award a person who suffers an ascertainable financial or property loss as a result of a violation of the Act threefold their actual damages, plus fees and costs. But *see Holmes v. Countrywide Financial Corp.*, No. 5:08-CV-00205-R, 2012 WL 2873892 at *13 (July 12, 2012) (declining to find a private right of action).
Credit Monitoring Required	—

New Mexico

State and Statute	N.M. Stat. 57-12C-1 et seq.
Covered Entities	A person that owns or licenses or maintains elements that include personal identifying information of a New Mexico resident.
Definition of Personal Information	An individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable: • Social Security Number • Driver's License Number • Government-issued identification number • Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account • Biometric data *Exceptions:* Information lawfully obtained from publicly available sources or from federal, state, or local government records lawfully made available to the general public.
Definition of Breach	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. Does not include the good-faith acquisition of personal information by an employee or agent of a business.
Threshold for Notification	A person that owns or licenses elements that include personal, identifying information of a New Mexico resident shall provide notification to each New Mexico resident whose personal, identifying information is reasonably believed to have been subject to a security breach. Any person that is licensed to maintain or possess computerized data containing personal, identifying information of a New Mexico resident that the person does not own or license shall notify the owner or licensee of the information of any security breach. No notice is required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.

Notification of Data Subject	Yes, notice to affected persons must include the following information: • The name and contact information of the notifying person; a list of the types of personal, identifying information that is reasonably believed to have been the subject of the breach, if known • The date, estimated date, or date range within which the breach occurred; a general description of the incident • Toll-free numbers and addresses of the major consumer reporting agencies • Advice directing the individual to review personal account statements and credit reports to detect errors resulting from the incident • A statement informing the individual of their rights under the Fair Credit Reporting and Identity Security Act
Notification of Government	Yes, if notice must be provided to more than 1,000 New Mexico residents as a result of a single security breach shall notify the office of the attorney general in the most expeditious time possible, and no later than 45 calendar days. Any person who maintains or possesses computerized data containing New Mexico residents' personal identifying information they do not own must notify the owner or licensee of the breach in the most expeditious time possible, but no later than 45 days after discovering the breach.
Notification of Credit Reporting Agencies	Credit agency reporting required if notice must be provided to more than 1,000 New Mexico residents as a result of a single security breach in the most expeditious time possible, and no later than 45 calendar days.
Notification by Third Parties	—
Timing of Notification	In the most expeditious time possible, but no later than 45 days following discovery of the breach. Notice may be delayed: • if a law enforcement agency determines that the notification will impede a criminal investigation • as necessary to determine the scope of the security breach and restore the integrity, security, and confidentiality of the data system
Form of Notification	Written or electronic (if electronic, consistent with 15 U.S.C. § 7001). Or substitute notice, if the cost of notification exceeds $100,000, the number of affected individuals is greater than 50,000, or the business has insufficient information for the other forms of notice. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to statewide media and Attorney General

Exemptions or Safe Harbors	Following entity's own notification procedures consistent with the statute. *Exemptions:* A person subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996. The State of New Mexico and it's political subdivisions are exempt from the provisions of this Act.
Consequences of Non-Compliance	*Government enforcement?* By the Attorney General. The court may: • Issue an injunction • Award damages for actual costs or losses, including consequential financial losses If the court determines that a person violated the Data Breach Notification Act knowingly or recklessly, the court may impose a civil penalty of the greater $25,000 or, in the case of failed notification, $10.00 per instance of failed notification with a maximum of $150,000. *Private right of action?* No.
Credit Monitoring Required	—

New York

State and Statute	New York Gen. Bus. Law § 899-aa; State Tech Law § 202 et seq. State Tech Law § 202 et seq.
Covered Entities	Any person, business, or state agency that owns, maintains, or licenses private information. State agency is defined as any state office or other governmental entity performing a governmental or proprietary function for the State of New York, except the judiciary, state legislature, any unit of local government, and district attorneys' offices. The terms person and business are not defined.
Definition of Personal Information	Definition of "personal information": Any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. Definition of "private information" – either: Personal information combined with one or more of the following, when either the data element or the combination of personal information plus the data element is not encrypted, or the encryption key has been acquired by an unauthorized individual: • Social Security Number • Driver's License Number • Account, credit card, or debit card number, along with any required access code needed to access the 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, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voiceprint, retina or iris image, or other unique physical representation or digital representation of biometric data that is used to authenticate or ascertain the individual's identity • A username or e-mail address in combination with a password or security question and answer that would permit access to an online account *Exception:* Information that is lawfully obtained from publicly available sources including the federal, state or local government records.
Definition of Breach	An unauthorized access to or acquisition of computerized data that compromises the security, confidentiality, or integrity of private information. This does not include the good-faith acquisition of personal information by an employee or agent of a business.

Threshold for Notification	Discovery or notification of the breach. Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the state entity reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affected over 500 residents of NY, the state entity shall provide the written determination to the state attorney general within ten days after the determination.
Notification of Data Subject	Yes, any person or business that owns or licenses computerized data, which includes private information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. An entity that maintains data on behalf of another must notify the other immediately after discovering a breach, if it is reasonably believed that there was unauthorized access to or acquisition of private information.
Notification of Government	Yes, if any NY residents are notified the state Attorney General must be notified and provided with a copy of the template notice to be provided to residents.
Notification of Credit Reporting Agencies	Credit agency reporting required if more than 5,000 NY residents are notified.
Notification by Third Parties	—
Timing of Notification	The most expeditious time possible and without unreasonable delay. Consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach.
Form of Notification	Written, telephonic, or electronic (if electronic, there must be express consent for electronic notice). Or substitute notice, if the cost of notification exceeds $250,000, the number of affected individuals is greater than 500,000, or the business has insufficient information for the other forms of notice. Substitute notice must consist of: • Email, unless the breached information includes an email along with a password or security question that would permit access to the account • Conspicuous posting on business's website • Notification to statewide media

Exemptions or Safe Harbors	Additional notice not required if notice given under GLBA, HIPAA, or part 500 of title XXIII of the official compilation of codes, rules, and regulations of the State of New York or any other data security rules administered by New York State.
Consequences of Non-Compliance	*Government enforcement?* Enforced by the Attorney General, including equitable relief, fines up to $250,000, and costs to persons to whom notice was not provided. *Private right of action?* Yes, suits must be brought within two years of the act complained of or the date of discovery.
Credit Monitoring Required	—

North Carolina

State and Statute	North Carolina Gen. Stat. Ann. §§ 75-60, 75-65
Covered Entities	Businesses, however organized, both for-profit and not for-profit, that own or license personal information of state residents. Does not include any government agency or division. Duties cannot be waived.
Definition of Personal Information	A person's first name or first initial and last name in combination with: • Social Security or employer taxpayer identification numbers • Driver's license, state identification card, or passport numbers • Checking account numbers • Savings account numbers • Credit card numbers • Debit card numbers • Personal Identification Number (PIN) Code as defined in G.S. 14-113.8(6) • Digital signatures • Any other numbers or information that can be used to access a person's financial resources • Biometric data • Fingerprints Does not include the following information unless it would permit access to a person's financial account or resources: • Electronic identification numbers • Electronic mail names or addresses • Internet account numbers • Internet identification names • Parent's legal surname prior to marriage • Passwords Does not include information that is lawfully obtained from publicly available sources.
Definition of Breach	An unauthorized access to and acquisition of unencrypted and un-redacted 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. This does not include the good-faith acquisition of personal information by an employee or agent of a business.

Threshold for Notification	Discovery or notification of the breach.
Notification of Data Subject	Yes, notice to affected persons must be clear and conspicuous and include at least the following elements: • A general description of the incident • Description of the types of personal information accessed in the breach • Description of the general actions the covered entity has taken to protect personal information from further unauthorized access • A business telephone number, if one exists, that affected persons can call for further information and assistance • Advice directing affected persons to remain vigilant in monitoring their account statements and credit reports • The major consumer reporting agencies' toll-free telephone numbers and addresses • A statement that affected persons can obtain information about preventing identity theft from and the toll-free telephone numbers, addresses, and website addresses for the Federal Trade Commission and the North Carolina Attorney General's Office Any business that possesses records containing PI of residents of NC that the business does not own or license or conducts business in NC that possesses records containing PI that the business does not own or license, shall notify the owner or licensee of the PI of any security breach immediately following discovery of the breach.
Notification of Government	Yes, must notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office.
Notification of Credit Reporting Agencies	Credit agency reporting required if more than 1,000 persons are notified under this section.
Notification by Third Parties	—
Timing of Notification	Without unreasonable delay, consistent with the legitimate needs of law enforcement. Consistent with the legitimate needs of law enforcement, any measures necessary to determine sufficient contact information, and to determine the scope of the breach.

Form of Notification	Written, telephonic, or electronic (if electronic, consistent with 15 U.S.C. § 7001). Or substitute notice, if the cost of notification exceeds $250,000, the number of affected individuals is greater than 500,000, or the business has insufficient information for the other forms of notice. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to statewide media
Exemptions or Safe Harbors	Financial institutions and credit unions in compliance with regulations as laid out in the statute.
Consequences of Non-Compliance	*Government enforcement?* The Attorney General has civil enforcement authority and may pursue a civil penalty up to $5,000 for knowing violations. The Attorney General may also seek criminal penalties. *Private right of action?* Yes, an individual injured as a result of a violation may institute a civil action. An injured person may seek injunctive relief and treble damages, and the court may award prevailing party attorneys' fees.
Credit Monitoring Required	—

North Dakota

State and Statute	North Dakota N.D. CENT. CODE § 51-30-01 et seq.
Covered Entities	Any person or service provider conducting business in North Dakota who owns, licenses, or maintains computerized data that includes personal information must notify the owner or licensor of any breach immediately following discovery.
Definition of Personal Information	An individual's first name or initial and last name, in conjunction with any of the following: • Social Security number • Driver's license or state ID number • Financial institution, credit, and debit card account numbers • Date of birth • Health insurance or medical information • Employer ID, or digitized or electronic signature "Personal information" does not include publicly available information lawfully obtained from federal, state, or local government records.
Definition of Breach	An unauthorized acquisition of computerized data entailing personal information, when access has not been secured by encryption that renders the data unusable. Good-faith acquisition of an individual's personal information by an employee or agent of the individual is not a breach, provided the data is not used or subject to further unauthorized disclosure.
Threshold for Notification	Possessors or licensors of computerized data containing personal information must disclose breaches to residents whose personal information was, or is reasonably believed to have been, acquired by an unauthorized individual. Disclosure may be delayed pending a determination of the scope of the breach and steps to remedy the disclosure, and if a law enforcement agency determines that disclosure would impede a criminal investigation.
Notification of Data Subject	Yes, covered entities shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of ND whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person. Any persons maintaining computerized personal data on behalf of another must notify the owner or licensee of any breach immediately, if the personal information is reasonably believed to have been acquired by an unauthorized person.
Notification of Government	Yes, if more than 250 individuals are notified.
Notification of Credit Reporting Agencies	—

Notification by Third Parties	—
Timing of Notification	In the most expeditious time possible and without unreasonable delay, but subject to delay to accommodate the needs of a law enforcement agency to conduct a criminal investigation.
Form of Notification	By one of the following: • Written notice • Electronic notice as long as it comports with the provisions of 15 U.S.C. § 7001 • Substitute notice in certain circumstances Substitute notice is appropriate if the cost of providing written or electronic notice would exceed $250,000, or the affected class exceeds 500,000 individuals, or if the possessor or licensor does not have sufficient contact information for the affected class. Substitute notice consists of the following: • Email notice when possible • Conspicuous posting of the notice on the possessor or licensor's webpage • Notification to major statewide media
Exemptions or Safe Harbors	An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information, with timing requirements that are consistent with this statute and comply with this statute's notification requirements. Following agency guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice. A covered entity subject to 45 C.F.R. § 164.402, which prescribes notification procedures for breaches of protected health information, is deemed to be in compliance with this chapter.
Consequences of Non-Compliance	*Government enforcement?* The Attorney General may impose civil penalties of not more than $5,000 for each violation. *Private right of action?* No.
Credit Monitoring Required	—

Ohio

State and Statute	Ohio REV. CODE ANN. § 1349.19 et seq.
Covered Entities	Any individual or business entity that owns or licenses computerized data that includes personal information.
Definition of Personal Information	An individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: • Social Security number • Driver's license number or state ID number • Financial, credit, or debit card account number in combination with any security code or password that would permit access to the individual's financial account "Personal information" does not include publicly available information lawfully obtained from federal, state, or local government records, or any information gathered from news organizations or nonprofit associations.
Definition of Breach	Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person, where access must be believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of Ohio. Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach.
Threshold for Notification	Must disclose any breach of the security of a system following discovery or notification of a breach to any Ohio resident whose personal information was or reasonably is believed to have been accessed or acquired by an unauthorized person if the access or acquisition causes or is reasonably believed to cause a material risk of identity theft or other fraud to the individual whose personal information was disclosed.
Notification of Data Subject	Yes, and any entity that maintains personal information on behalf of another entity, must notify any such entity as expeditiously as possible when it learns of a breach involving personal information owned by the other entity.
Notification of Government	—

Notification of Credit Reporting Agencies	Credit agency reporting required if more than 1,000 Ohio residents are required to be notified as a result of being involved in a single occurrence of a breach of the security of the system.
Notification by Third Parties	—
Timing of Notification	Notice must be made within 45 days following discovery or notification of the breach, subject to any measures necessary to determine the scope of the breach and restore the integrity of the system. Notice may be delayed if a law enforcement agency determines that it would impede a criminal investigation or jeopardize homeland or national security.
Form of Notification	Notice may be provided by one of the following • Written notice • Electronic notice • Telephone notice • Substitute notice in certain circumstances Substitute notice is permissible if the cost of providing written or electronic notice would exceed $250,000, or the affected class exceeds 500,000 individuals, or if the possessor or licensor does not have sufficient contact information for the affected class. Substitute notice consists of: • Email notice when possible • Conspicuous posting of the notice on the possessor or licensor's webpage • Notification to major media outlets in the area in which the business entity is located Alternative substitute notice is available if affected entity has less than ten employees and the cost of notice would exceed $10,000, and consists of: • Notification by paid advertisement in a local newspaper that covers at least one-quarter of a page and published at least once a week for three consecutive weeks • Conspicuous posting of a disclosure on the entity's website • Notification to major media outlets in the Entity's geographic area

Exemptions or Safe Harbors	Covered entities (businesses that access, maintain, communicate, or process personal information or restricted information in or through one or more systems, networks, or services located in or outside Ohio) may claim an affirmative defense against certain breach claims if they develop a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conform to an industry-recognized cybersecurity framework; or that create such a program for the protection of both personal information and restricted information. A financial institution, trust company, or credit union or any affiliate that is required by federal law to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency is exempt from this section. A covered entity subject to 45 C.F.R. § 160, which prescribes notification procedures for breaches of protected health information, is deemed to be in compliance with this chapter. Disclosure may be made pursuant to the terms of a contract with a separate entity if the contract does not conflict with a provision of this statute.
Consequences of Non-Compliance	State attorney general may conduct an investigation and impose civil penalties.
Credit Monitoring Required	—

Oklahoma

State and Statute	Oklahoma STAT. tit. 24 § 161 et seq.
Covered Entities	Corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or any other profit or non-profit entity that owns or licenses computerized data containing personal information of Oklahoma residents.
Definition of Personal Information	The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of Oklahoma, when the data elements are neither encrypted nor redacted, and the information is not otherwise lawfully obtained or publically available: • Social Security Number • Driver's license or state ID number • Financial, credit card, or debit card account number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident *Exception* The term does not include publicly available information including that from federal, state or local government records.
Definition of Breach	An unauthorized access and acquisition of unencrypted and non-redacted computerized data that compromises the security or confidentiality of personal information and causes, is reasonably believed has caused, or will cause identity theft or other fraud. Good-faith acquisition of personal information by an employee or agent of an individual or entity is not a breach, provided that the personal information is not used unlawfully or subject to unauthorized disclosure.
Threshold for Notification	A breach must be disclosed if personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person, and the access or acquisition causes, is believed to have caused, or will cause identity theft or other fraud.
Notification of Data Subject	Yes, and an individual or entity that maintains computerized personal information on behalf of another entity shall notify the data's owner or licensee of any breach as soon as practicable following discovery, if the data is reasonably believed to have been acquired by an unauthorized person.
Notification of Government	No, unless business is subject to oversight of state Real Estate Commission.
Notification of Credit Reporting Agencies	—

Notification by Third Parties	—
Timing of Notification	Disclosure should be made without unreasonable delay and as soon as practicable after discovery or notification of a breach. Disclosure may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security.
Form of Notification	Notification may be provided by: • Written notice to the postal address in the records of the individual or entity • Telephone notice • Electronic notice • Substitute notice in certain circumstances Substitute notice is permissible where the individual or entity can demonstrate that the cost of providing notice will exceed $50,000 or that the affected class of Oklahoma residents exceeds 100,000 persons, or if the individual or entity does not have sufficient contact information or consent to provide other types of notice, and consists of any two of the following: • Email notice where available • Conspicuous posting of the notice of the website of the individual or entity • Notice to major statewide media
Exemptions or Safe Harbors	An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information, with timing requirements that are consistent with this statute and comply with this statute's notification requirements. A financial institution that complies with the notification requirements of the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this statute. An entity that complies with the notification requirements established by its primary federal regulator is deemed to be in compliance with this statute.
Consequences of Non-Compliance	State Attorney General or district attorney enforcement. Penalties include actual damages for a violation or a civil penalty not to exceed $150,000 per breach (or series of similar breaches). A violation by a state-chartered or licensed financial institute is enforceable exclusively by the primary state regulator of the institution.
Credit Monitoring Required	—

Oregon

State and Statute	Oregon REV. STAT. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626
Covered Entities	Any individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization or other entity, whether or not organized to operate at a profit, or a public body that owns, maintains, or otherwise possesses data that includes a state resident's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities. Also applies to any entities that maintain, store, or process information on their own behalf, but that they do not own.
Definition of Personal Information	Consumer's first name or first initial and last name in combination with any one or more of the following unencrypted, non-redacted, and unprotected data elements: • Social Security Number • Driver's license or state ID number • Passport number or other identification number issued by the United States • A consumer's financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account • 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 • A consumer's 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 • Any 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 • Any of the aforementioned data elements alone or in combination if encryption or redaction techniques have not been used and the information obtained would be sufficient to permit a person to commit identify theft against the state resident whose information was compromised This definition does not include any data in a federal, state, or local government record lawfully made available to the public.
Definition of Breach	An unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information that a person maintains. Definition does not include an inadvertent acquisition of personal information by a person or the person's employee or agent if the personal information is not used unlawfully or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

Threshold for Notification	Following discovery or receipt of notification of a breach, any person that owns, maintains, or otherwise possesses data containing personal information must give notification to affected consumers. A person that maintains or otherwise possesses personal information on behalf of, or under license of, another person shall notify the other person after discovering a breach of security. If, after an investigation or consultation with relevant federal, state, or local law enforcement agencies, the covered entity determines that no reasonable likelihood of harm to the consumers has resulted or will result, no notification is required. Such a determination must be documented in writing and maintained for five years. This section does not apply to: • Any person who complies with notification requirements promulgated by a primary federal regulator, as long as those requirements are as stringent as the requirements in this section • A person that complies with a state or federal law providing greater protection to personal information and disclosure requirements at least as thorough as those in this section • A person subject to and compliant with Title V of the Gramm-Leach-Bliley Act Except as provided below, a covered entity, as defined in 45 C.F.R. 160.103, as in effect on January 1, 2016, that is governed under 45 C.F.R. parts 160 and 164, as in effect on January 1, 2016, if the covered entity sends the Attorney General a copy of the notice the covered entity sent to consumers under ORS 646A.604 or a copy of the notice that the covered entity sent to the primary functional regulator designated for the covered entity under HIPAA. A covered entity is subject to this section if the covered entity does not send a copy of a notice described above to the Attorney General within a reasonable time after the Attorney General requests the copy.
Notification of Data Subject	Yes, and a person that maintains or otherwise possesses personal information on behalf of, or under license of, another person shall notify the other person after discovering a breach of security.
Notification of Government	Yes, state Attorney General must be notified if more than 250 residents are notified.
Notification of Credit Reporting Agencies	Credit agency reporting required if more than 1,000 residents are notified.

Notification by Third Parties	—
Timing of Notification	The disclosure notification must be made in the most expeditious time possible and without unreasonable delay. Delays consistent with the legitimate needs of law enforcement and any measures necessary to determine sufficient contract information for consumers, determine the scope of the breach, and restore the integrity and security of the data.

Form of Notification	Notification to the consumer may take the form of:
	• Written notice
	• Telephone notice provided that contact is made directly with the affected consumer, and must include at a minimum:
	  • A description of the incident in general terms
	  • The approximate date of the breach
	  • The type of personal information disclosed as a result of the breach
	  • Contact information of the person subject to this statute
	  • Contact information for national consumer reporting agencies
	  • Advice to the consumer to report suspected identify theft to law enforcement
	  • Electronic notice if customary and if consistent with the provisions of 15 U.S.C. § 7001
	  • Substitute notice, if the person demonstrates that the cost of providing notice would exceed $250,000 or if the affected class of consumers exceeds 350,000 consumers, or if the person does not have sufficient contact information to provide notice
	
	Substitute notice consists of:
	• Conspicuous posting of the notice or a link to the notice on the person's website
	• Notification to major statewide television and newspaper media

Exemptions or Safe Harbors	The notification requirements of the statute do not apply to a person that complies with security procedures that provide greater protection to personal information and comparably thorough disclosure requirements pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary federal regulator. The notification requirements also do not apply to a person that complies with a state or federal law that provides greater protection to personal information and comparably thorough disclosure requirements as this statute, as well as a financial institution subject to 15 U.S.C. § 6801 et seq. A person that owns a small business complies if the person's information security and disposal program contains administrative, technical, and physical safeguards and disposal measures appropriate to the size and complexity of the small business, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers.
Consequences of Non-Compliance	The Department of Consumer and Business Services may conduct a public or private investigation of any breach and issue cease and desist orders to violators. Any person who violates or procures, aids, or abets in a violation of this statute shall be subject to a penalty of not more than $1,000 for every violation. Each day's continuance is a separate violation, and the maximum penalty for any occurrence shall not exceed $500,000.
Credit Monitoring Required	—

Pennsylvania

State and Statute	Pennsylvania 73 PA. STAT. § 2301 et seq.
Covered Entities	Any state agency, political subdivision, or an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data that includes personal information of Pennsylvania residents.
Definition of Personal Information	The first name or first initial and last name of an individual when combined with and linked to any one or more of the following types of unencrypted, non-redacted data: • Social Security number • Driver's license or state ID number • Debit, credit, or financial account number in combination with any security code, access code, or password that would permit access to a person's financial account This category does not include information that is lawfully obtained from federal, state, or local government records available to the general public.
Definition of Breach	An unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information, where the access and acquisition cause, or are believed to have caused, a resident of Pennsylvania to become the victim of loss or injury. The definition of breach does not encompass good-faith acquisition of personal information by the individual or by an agent of the individual acting lawfully to acquire the individual's personal information.
Threshold for Notification	Covered entities must provide notice when they reasonably believe that the unencrypted and non-redacted personal information of a Pennsylvania resident was accessed or acquired by an unauthorized person, or where an unauthorized person accessed or acquired an encryption key.
Notification of Data Subject	Yes, any vendor that maintains, stores, or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores, or manages the data.
Notification of Government	No.
Notification of Credit Reporting Agencies	Credit agency reporting required when more than 1,000 residents are notified, and nationwide credit reporting agencies must be notified without unreasonable delay, regarding the timing, distribution, and number of consumer notices.
Notification by Third Parties	—

Timing of Notification	Notification of a breach shall be made without unreasonable delay, subject to the covered entity's need to take measures necessary to determine the scope of the breach and to restore integrity of the data system. Delay may be appropriate where a law enforcement agency determines and advises the covered entity in writing that notification would impede a criminal or civil investigation.
Form of Notification	Notice required by this section may be effected by: • Written notice to the last-known home address for the individual • Telephone notice, if the affected individual can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information, but does not require the affected individual to provide personal information, and the affected individual is provided with a telephone number to call or website to visit for further information or assistance • Email notice, if a prior business relationship exists and the covered entity has a valid email address for the affected individual • Substitute notice, in certain circumstances Substitute notice will be appropriate if the individual or entity demonstrates that the cost of providing notice will exceed $100,000 or that the class of affected individuals exceeds 175,000 persons, or that the individual or entity lacks sufficient contact information to provide notice to affected individuals, and consists of all of the following: • Email notice if the covered entity has email addresses for affected individuals • Conspicuous posting of the notice on the covered entity's website • Notification to major statewide media
Exemptions or Safe Harbors	A covered entity that maintains its own notification procedures as part of an information security policy is in compliance with the notification requirements of the statute if the timing requirements are consistent with the statute, and the entity provides notice in accordance with those policies in the event of a breach. A covered entity that complies with the notification requirements or procedures prescribed by the entity's primary federal regulator is deemed to be in compliance. A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance.

Consequences of Non-Compliance	Attorney General of Pennsylvania has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for violations of this section.
Credit Monitoring Required	—

Puerto Rico

State and Statute	Puerto Rico P.R. LAWS ANN. tit. 10, § 4051 et seq.
Covered Entities	Any entity that owns or serves as the custodian of a database that includes the personal information of residents of Puerto Rico, including agencies, boards, bodies, examining boards, corporations, public corporations, committees, independent offices, divisions, administrations, bureaus, departments, authorities, officials, public and private educational institutions, instrumentalities or administrative organisms of the three branches of government, corporations, partnerships, associations, private companies, or organizations authorized to do business in Puerto Rico.
Definition of Personal Information	At least the first name or first initial and last name of an individual when combined with one or more of the following types of unencrypted data, such that an association may be established between a name and an item of data: • Social Security number • Driver's license number, voter identification card, or other official identification • Bank and financial account numbers, either alone or in combination with access and security codes • Usernames and passwords or access codes to public or private information systems • HIPAA-protected information • Tax information • Work-related evaluations This category does not include information that is lawfully obtained from publicly available sources, nor does it include the residential address of any individual.
Definition of Breach	An unauthorized access—including electronic and physical access to data banks and recording media—that compromises the security, confidentiality, or integrity of data containing personal information, or when a covered entity knows or reasonably suspects that a normally authorized person who had access to the personal information violated its confidentiality or obtained the data through false representation with the intent to use it illegally.
Threshold for Notification	A covered entity must notify citizens of any breach of a security system when the breached database contains, in whole or in part, unencrypted personal information files that may or may not be password-protected.
Notification of Data Subject	Yes, and any entity that resells or provides access to digital data banks that contain personal information files of citizens must notify the custodian of said information of any breach that has allowed unauthorized access to those files.
Notification of Government	Yes, covered entities must report breaches to the Department of Consumer Affairs within 10 days of detection.

Notification of Credit Reporting Agencies	—
Notification by Third Parties	—
Timing of Notification	Covered entities must notify affected individuals as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as application of measures needed to restore the system's security. Covered entities must also provide notice to the Department of Consumer Affairs within 10 days of detection of a breach.
Form of Notification	Notice must be provided in a clear and conspicuous manner, and should describe the breach and the type of sensitive information compromised in general terms, as well as provide a toll free number and website for affected individuals to use for assistance and information. Notice may be effected by one of the following methods: • Written notice • Electronic notice, consistent with the requirements of the Digital Signatures Act • Substitute notice, in certain circumstances Substitute notice will be appropriate if the individual or entity demonstrates that the cost of providing notice is excessively onerous or will exceed $100,000 or that the class of affected individuals exceeds 100,000 persons, or if locating all of the members of the affected class is too difficult, and consists of two steps: 1. Prominent display of an announcement of the breach at the physical premises of the covered entity, on the website of the entity, and in informative flyers sent electronically or through regular mail; and 2. A communication to general or sector-specific media detailing the situation and providing contact information for affected individuals to use when seeking information or advice.
Exemptions or Safe Harbors	Institutional information and security policies that provide equal or better protection than this section are deemed to be in compliance.
Consequences of Non-Compliance	Civil penalties of up to $5,000 for each violation of this section. Private right of action for damages.
Credit Monitoring Required	—

Rhode Island

State and Statute	Rhode Island R.I. GEN. LAWS § 11-49.2-1 et seq.
Covered Entities	Any state agency, individual, partnership association, corporation or joint venture that owns, maintains, or licenses computerized data that includes personal information.
Definition of Personal Information	The first name or first initial and last name of an individual when combined with one or more of the following types of non-encrypted data: • Social Security number • Driver's license number or state ID number • Debit or credit card account number, in combination with any security code, access code, or password that would permit access to a person's financial account • Medical or health insurance information • Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account
Definition of Breach	An unauthorized access or acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity or state agency. Good-faith acquisition of personal information by an employee or agent of the state agency for lawful purposes does not constitute a breach, provided the personal information is not unlawfully used or subject to unauthorized disclosure.
Threshold for Notification	Following discovery or notification of a breach, a covered entity must notify any resident of Rhode Island whose personal information was, or is reasonably believed to have been acquired by an unauthorized person and subject to a risk of identity theft. Notification is not required if, after conducting an appropriate investigation or consulting with relevant federal, state, and local law enforcement agencies, a covered entity determines that the breach has not and will likely not result in a significant risk of identity theft to the affected individuals.
Notification of Data Subject	Yes.
Notification of Government	Yes, if more than 500 Rhode Island residents are notified.
Notification of Credit Reporting Agencies	Credit agency reporting required if more than 500 Rhode Island residents are notified.

Notification by Third Parties	—
Timing of Notification	Disclosure to affected individuals must be made in the most expeditious time possible and no later than 45 calendar days after confirmation of the breach, consistent with legitimate needs of law enforcement. Notification may be delayed if a law enforcement agency determines that it would impede a criminal investigation.
Form of Notification	Notice may be provided by any one of the following methods: • Written notice • Electronic notice, if consistent with the requirements of 15 U.S.C. § 7001 • Substitute notice, in certain circumstances Substitute notice will be appropriate if the state agency or covered entity demonstrates that the cost of providing notice would exceed $25,000 or that the class of affected individuals exceeds 50,000 persons, or that the covered entity or state agency lacks sufficient contact information to provide notice to affected individuals, and consists of all of the following: • Email notice if the covered entity or state agency has email addresses for affected individuals • Conspicuous posting of the notice on the covered entity or state agency's website • Notification to major statewide media
Exemptions or Safe Harbors	A covered entity that maintains its own notification procedures as part of an information security policy is in compliance with the notification requirements of the statute if the timing requirements are consistent with the statute and the entity provides notice in accordance with those policies in the event of a breach. A covered entity that complies with notification requirements established in the rules, regulations, or guidelines of its primary or functional regulator is deemed to be in compliance with this section. A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is deemed to be in compliance with this section. A financial institution, trust company, credit union or its affiliates that is in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this section.

Consequences of Non-Compliance	Each reckless violation is a civil violation for which a penalty of not more than $100 will apply. Each knowing and willful violation is a civil violation for which a penalty of not more than $200 will apply. Actions may be brought by the state Attorney General.
Credit Monitoring Required	—

South Carolina

State and Statute	South Carolina CODE ANN. § 39-1-90
Covered Entities	Any natural person, individual, corporation, government, or governmental subdivision or agency, trust estate, partnership, cooperative, or association conducting business in South Carolina and owning or licensing computerized data or other data that includes personal identifying information.
Definition of Personal Information	The first name or first initial and last name of an individual when combined with or linked to one or more of the following types of non-encrypted or non-redacted data: • Social Security number • Driver's license or state ID number • Financial, debit card, or credit card account number, in combination with any security code, access code, or password that would permit access to a person's financial account • Other numbers or information used (i) to access a person's financial accounts, or (ii) by a governmental or regulatory entity that will uniquely identify an individual This category does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records available to the general public.
Definition of Breach	An unauthorized access to and acquisition of unencrypted and non-redacted computerized data that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, and when illegal use of the information has occurred or is likely to occur, or where use of the information creates a material risk of harm to a resident. Good-faith acquisition of personal identifying information by an agent of employee of the person—when used for business purposes and when undisclosed to unauthorized individuals—does not constitute a breach.
Threshold for Notification	Following discovery or notification of a breach, a covered entity must provide notice to a resident of South Carolina whose non-redacted and unencrypted personal identifying information is acquired by an unauthorized person, and where illegal use of the information has occurred, is reasonably likely to occur, or creates a material risk of harm to the resident.
Notification of Data Subject	Yes, and third parties doing business in the state and handling or maintaining electronic personal data that they do not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Government	Yes, must notify Consumer Protection Division of Consumer Affairs department if more than 1,000 state residents are notified.

Notification of Credit Reporting Agencies	Nationwide credit reporting agencies must be notified of the timing, distribution, and content of the notice if more than 1,000 state residents are notified.
Notification by Third Parties	—
Timing of Notification	Disclosure must be made in the most expeditious time possible and without unreasonable delay, consistent with (i) the needs of law enforcement agencies in conducting a criminal investigation and (ii) with measures necessary to determine the scope of the breach and restore the integrity of the data system.
Form of Notification	Notice may be provided by one of the following methods: • Written notice • Telephonic notice • Electronic notice, consistent with the requirements of 15 U.S.C. § 7001 • Substitute notice, in certain circumstances Substitute notice will be appropriate if the covered entity demonstrates that the cost of providing notice will exceed $250,000 or that the class of affected individuals exceeds 500,000 persons, or if the covered entity lacks sufficient contact information to provide notice to affected individuals, and consists of: • Email notice if the covered entity has email addresses for affected individuals • Conspicuous posting of the notice on the covered entity's website • Notification to major statewide media
Exemptions or Safe Harbors	A covered entity that maintains its own notification procedures as part of an information security policy is in compliance with the notification requirements of the statute if the timing requirements are consistent with the statute and the entity provides notice in accordance with those policies in the event of a breach. A bank or financial institution in compliance with the Gramm-Leach-Bliley Act is deemed to be in compliance with this section. A financial institution subject to and in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this section.
Consequences of Non-Compliance	Department of Consumer Affairs can impose administrative penalties of up to $1,000 per affected resident for knowing and willful violations of this section. Private right of action for damages or injunction.
Credit Monitoring Required	—

South Dakota

State and Statute	South Dakota
Covered Entities	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 ("Information Holder").
Definition of Personal Information	"Personal Information" means a person's first name or first initial and last name, in combination with any one or more of the following data elements: • Social Security number • Driver's license number or any other unique identification number created or collected by a government body • Account number or credit card number or debit card number in combination with any required security code, access code, password, routing number, PIN, or any additional information that is necessary to access the financial account • Health information as defined in 45 CFR 160.103 (HIPAA) • An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes The term does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable. "Protected Information" includes: • A username or email address, in combination with a password, security question answer, or other information that permits access to an online account • Account number or credit and debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account
Definition of Breach	An 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. Good-faith acquisition of personal or protected information by an employee or agent of an Information Holder is not a security breach, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Threshold for Notification	Any Information Holder that discovers or is notified of a breach of system security must notify affected individuals. Notice is not required if, following appropriate investigation and notification to the Attorney General, the Information Holder reasonably believes the incident will not result in harm to affected individuals. The Information Holder shall document this determination in writing and keep a record of this documentation for three years.
Notification of Data Subject	Yes.
Notification of Government	If the number of affected individuals exceeds 250 residents, the Information Holder must notify the Attorney General.
Notification of Credit Reporting Agencies	The Information Holder must notify, without unreasonable delay, all consumer reporting agencies and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis.
Notification by Third Parties	—
Timing of Notification	Notice must be given no later than 60 days from when the Information Holder discovers or is notified of a breach.
Form of Notification	Notice may be provided by one of the following methods: • Written notice • Electronic notice, if the electronic notice is consistent with the requirements for electronic records and signatures set forth in 15 U.S.C. § 7001, (E-SIGN ACT) or if the information holder's primary method of communication with the SD resident has been by electronic means Substitute notice is acceptable if notification will exceed $250,000, the affected class of persons to be notified exceeds 500,000 persons, or the information holder does not have sufficient contact information and the notice consists of each of the following: • Email notice, if the information holder has the affected individual's email address • Conspicuous posting of the notice on the website of the Information Holder if it has a website; and notification to statewide media

Exemptions or Safe Harbors	An Information Holder subject to or regulated by federal laws, rules, regulations, procedures, or guidance (including GLBA and HIPAA) is considered in compliance with the Act as long as the Information Holder maintains procedures pursuant to the federal law requirements and provides notice to consumers pursuant to those requirements. An Information Holder that maintains its own notification procedure as part of its information security policy, and the policy is consistent with the timing requirements of the Act, is considered in compliance with the notification requirements of this Act if it notifies affected persons in accordance with its internal policy.
Consequences of Non-Compliance	Attorney General may prosecute violations as an unfair or deceptive act or practice under state law, and may bring an action to recover on behalf of the state a civil penalty of not more than $10,000 per day per violation. The attorney general may recover attorneys' fees and any costs associated with any action brought under this section.
Credit Monitoring Required	—

Tennessee

State and Statute	Tennessee CODE ANN. § 47-18-2107
Covered Entities	Any person, business conducting business in Tennessee, agency of the State of Tennessee, or any of its political subdivisions owning or licensing computerized data that includes personal information.
Definition of Personal Information	The first name or first initial and last name of an individual when combined with one or more of the following types of non-encrypted data: • Social Security number • Driver's license number • Financial, debit card, or credit card account number, in combination with any security code, access code, or password that would permit access to a person's financial account This category does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records available to the general public.
Definition of Breach	An unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. Good-faith acquisition of personal information by an employee or agent of the information holder, for the purposes of the information holder, does not constitute a breach if the personal information is not used unlawfully or subject to unauthorized disclosure.
Threshold for Notification	Following discovery of a breach, any covered entity must immediately notify affected individuals if personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Data Subject	Yes, and an entity that maintains computerized data that includes personal information that the entity does not own must notify the owner or licensee of the information of any breach of the security of the data if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than 45 days from the discovery or notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement.
Notification of Government	—
Notification of Credit Reporting Agencies	If more than 1,000 residents are notified, nationwide credit reporting agencies must be notified without unreasonable delay, regarding the timing, distribution, and content of the notices.

Notification by Third Parties	—
Timing of Notification	Disclosure must be made in the most expeditious time possible and without unreasonable delay, subject to the legitimate needs of a law enforcement agency conducting a criminal investigation, and subject to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
Form of Notification	Notice may be provided by one of the following methods: • Written notice • Electronic notice, consistent with the requirements of 15 U.S.C. § 7001 • Substitute notice, in certain circumstances Substitute notice will be appropriate if the covered entity demonstrates that the cost of providing notice will exceed $250,000 or that the class of affected individuals exceeds 500,000 persons, or if the covered entity lacks sufficient contact information to provide notice to affected individuals, and consists of all of the following: • Email notice if the covered entity has email addresses for affected individuals • Conspicuous posting of the notice on the covered entity's website • Notification to major statewide media
Exemptions or Safe Harbors	A covered entity that maintains its own notification procedures as part of an information security policy is in compliance with the notification requirements of the statute if the timing requirements are consistent with the statute and the entity provides notice in accordance with those policies in the event of a breach. This statute does not apply to any covered entity that is subject to the provisions of Title V of the Gramm-Leach-Bliley Act. This statute does not apply to a covered entity subject to the Health Insurance Portability and Accountability Act. A financial institution subject to and in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this section.
Consequences of Non-Compliance	Private right of action for damages or injunction. The rights and remedies available under this section are cumulative to each other and to other legal rights and remedies.
Credit Monitoring Required	—

Texas

State and Statute	Texas BUS & COM. CODE ANN. §§ 521.002 et seq.
Covered Entities	A person conducting business in Texas that owns or licenses computerized data that includes sensitive personal information.
Definition of Personal Information	'Sensitive personal information' means unencrypted first name or first initial and last name of an individual when combined with or linked to one or more of the following types of unencrypted data: • Social Security number • Driver's license number or government-issued ID number • Financial, debit card, or credit card account number, in combination with any security code, access code, or password that would permit access to a person's financial account • Information identifying an individual and relating to the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual This category does not include information that is lawfully obtained from federal, state, or local government records available to the general public. 'Personal identifying information' means an individual's: • name, social security number, date of birth, or government-issued identification number • mother's maiden name • unique biometric data, including the individual's fingerprint, voiceprint, and retina or iris image • unique electronic identification number, address or routing code • telecommunication access device
Definition of Breach	The unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person, including data that is encrypted if the unauthorized individual obtains the encryption key. Good-faith acquisition of personal information by an employee or agent of the person, for the purposes of the person, does not constitute a breach unless the employee or agent uses or discloses the sensitive personal information in an unauthorized manner.
Threshold for Notification	After discovery or notification of a breach, a covered entity must notify any person, including nonresidents, whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification of Data Subject	Yes, and any entity that maintains computerized data that includes sensitive personal information that the entity does not own shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Government	Yes. Any entity that is required to provide notification of a security breach to at least 250 Texas residents, must notify the attorney general of that breach not later than 60 days after discovering the breach. The notification must include: • a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach • the number of Texas residents affected by the breach at the time of notification • the measures taken by the entity regarding the breach • any measures the entity intends to take regarding the breach after notification • information regarding whether law enforcement is investigating the breach
Notification of Credit Reporting Agencies	If an entity must notify at one time more than 10,000 persons of a breach of system security, it must also notify, without unreasonable delay, all consumer reporting agencies that maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices.
Notification by Third Parties	—
Timing of Notification	The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, consistent with the legitimate needs of law enforcement, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. A covered entity may delay providing notice at the request of a law enforcement agency that determines that notification will impede a criminal investigation. The required notification shall be made as soon as the law enforcement agency determines that the required notice will not compromise the investigation.

Form of Notification	A person may give notice by providing: • Written notice at the last-known address of the affected individual • Electronic notice, consistent with the requirements of 15 U.S.C. § 7001 • Substitute notice, in certain circumstances Substitute notice will be appropriate if the covered entity demonstrates that the cost of providing notice will exceed $250,000 or that the class of affected individuals exceeds 500,000 persons, or if the covered entity lacks sufficient contact information to provide notice to affected individuals, and consist of: • Electronic notice if the covered entity has email addresses for affected individuals • Conspicuous posting of the notice on the covered entity's website • Notice published in or broadcast on major statewide media
Exemptions or Safe Harbors	A covered entity that maintains its own notification procedures as part of an information security policy is deemed to be in compliance with the notification requirements of the statute if the timing requirements are consistent with the statute and the entity provides notice in accordance with those policies in the event of a breach.
Consequences of Non-Compliance	Enforcement by Texas Attorney General: • Injunctive or equitable relief • Attorney General is entitled to recover reasonable expenses for attorneys' fees, court costs, and investigatory costs Civil fines ranging from $2,000 to $50,000 per violation penalty of $100 per day that the covered entity fails to provide notification to an affected individual, up to $250,000.
Credit Monitoring Required	

US Virgin Islands

State and Statute	US Virgin Islands CODE ANN. tit. 14, §§ 2208-2212
Covered Entities	Any person or business that conducts business in the Virgin Islands and owns or licenses computerized data that includes personal information.
Definition of Personal Information	A person's unencrypted first name or first initial and last name, combined with any one or more of the following unencrypted or unprotected data elements relating to that person: • Social Security number • Driver's license number • Financial, credit card, or debit card account numbers in combination with any required security or access code, or password that would permit access to the person's financial account Information contained in federal, state, or local government records or that is lawfully made available to the general public does not constitute personal information.
Definition of Breach	An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. Good-faith acquisition of personal information by an employee or agent of the person, for the purposes of the person or business, does not constitute a breach provided the personal information is not unlawfully used or subject to further unauthorized disclosure.
Threshold for Notification	Following discovery or notification of a breach, a covered entity must notify any resident of the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Data Subject	Yes, and any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Government	No.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	—

Timing of Notification	Disclosure must be made in the most expeditious time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement agencies conducting a criminal investigation, and consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
Form of Notification	Notice may be provided by one of the following methods: • Written notice • Electronic notice, if consistent with the requirements of 15 U.S.C. § 7001 • Substitute notice, in certain circumstances Substitute notice will be appropriate if the covered entity demonstrates that the cost of providing notice will exceed $100,000 or that the class of affected individuals exceeds 50,000 persons, or if the covered entity lacks sufficient contact information to provide notice to affected individuals, and consists of: • Email notice if the covered entity has email addresses for affected individuals • Conspicuous posting of the notice on the covered entity's website • Notification to major territory-wide media
Exemptions or Safe Harbors	A covered entity that maintains its own notification procedures as part of an information security policy is deemed to be in compliance with the notification requirements of the statute if the timing requirements are consistent with the statute and the entity provides notice in accordance with those policies in the event of a breach.
Consequences of Non-Compliance	Private right of action for damages or injunction. The rights and remedies available under this section are cumulative to each other and to any other legal rights and remedies.
Credit Monitoring Required	—

Utah

State and Statute	Utah CODE ANN. §§ 13-44-101-103, 13-44-201-202, 13-44-301
Covered Entities	Any person who owns or licenses computerized data that includes personal information concerning a resident of Utah.
Definition of Personal Information	A person's unencrypted first name or first initial and last name, combined with any one or more of the following unencrypted or unprotected data elements relating to that person when either the name or data element is unencrypted or not protected by another method rendering the data unreadable or unusable: • Social Security number • Driver's license or state ID number • Financial, credit card, or debit card account numbers • Any required security or access code, or password that would permit access to the person's account Information contained in federal, state, or local government records or in widely distributed media that is lawfully made available to the general public does not constitute personal information.
Definition of Breach	An unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. An acquisition of personal information by an employee or agent of the person possessing unencrypted data does not constitute a breach, unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.
Threshold for Notification	A covered entity must provide notice to each affected Utah resident if, after learning of a breach and conducting a reasonable and prompt investigation in good faith, the entity determines that the disclosed personal information has been or will be misused for identity theft or fraudulent purposes.
Notification of Data Subject	Yes, and an entity that maintains computerized data that includes personal information that the entity does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the entity's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur.
Notification of Government	No.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	—

Timing of Notification	Following discovery or notification of a breach, a covered entity must provide notice in the most expeditious time possible and without unreasonable delay after determining the scope of the breach and after restoring the reasonable integrity of the data system. Delaying notification may be appropriate where a law enforcement agency determines that it may impede a criminal investigation.
Form of Notification	A person may give notice by providing: • Written notice by first-class mail to the most recent address of the affected individual • Electronic notice, if the primary method of communication with affected individuals is by electronic means, and consistent with the requirements of 15 U.S.C. § 7001 • Telephonic notice • By publishing notice of a breach in a newspaper of general circulation and fulfilling the requirements of Utah's legal notice publication requirements
Exemptions or Safe Harbors	A covered entity that maintains its own notification procedures as part of an information security policy is deemed to be in compliance with the notification requirements of the statute if the timing requirements are consistent with the statute and the entity provides notice in accordance with those policies in the event of a breach. A covered entity that is regulated by state or federal law is deemed to be in compliance with this section where it maintains procedures for a breach of system security under applicable law established by its primary state or federal regulator, and where it notifies each affected Utah resident in accordance with such a regulatory regime.
Consequences of Non-Compliance	Utah Attorney General: • Investigation and adjudication of violations. • Civil fines up to $2,500, but not greater than $100,000 for a violation or series of violations. • No private right of action, but covered entity may still be liable under independent contract or tort duties.
Credit Monitoring Required	—

Vermont

State and Statute	Vermont STAT. ANN. tit. 9 §§ 2430, 2435
Covered Entities	Any data collector, including but not limited to 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 entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with, owns, or licenses nonpublic computerized personal information concerning an individual living in Vermont.
Definition of Personal Information	A person's unencrypted first name or first initial and last name, combined with any one or more of the following unencrypted or unprotected data elements relating to that person that are not publicly available: • Social Security number • Motor vehicle operator's license number or non driver identification card number • Financial, credit card, or debit card account numbers if circumstances exist in which the number could be used without additional identifying information • Any required security or access code, or password that would permit access to the person's account Does not mean publicly available information that is available from federal, state or local government records.
Definition of Breach	An 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. In determining whether this definition applies, a covered entity may consider indications that information is in physical possession and control of an unauthorized person, that the information has been downloaded or copied, that the information was used by an unauthorized person, or that the information has been made public. A good-faith but unauthorized acquisition of personally, identifiable information by an employee or agent of the data collector, for a legitimate purpose, does not constitute a breach where the information is not subject to further unauthorized disclosure and is not used for a purpose unrelated to the data collector's business.
Threshold for Notification	Following discovery or notification of a breach, a covered entity must notify affected individuals who are residents of Vermont. Notice of a breach is not required if the covered entity demonstrates that misuse of personal information is not reasonably possible, and conveys that conclusion and an explanation to the Vermont Attorney General or (if registered thereunder) to the Department of Banking, Insurance, Securities, and Health Care Administration.

Notification of Data Subject	Yes, and any entity that maintains or possesses computerized data containing personal information of an individual residing in Vermont that the entity does not own or license or any entity that conducts business in Vermont that maintains or possesses records or data containing personal information that the entity 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.
Notification of Government	Yes. An entity shall notify the Attorney General or Department of Financial Regulation of any breach within 14 business days of the date the entity discovers the breach or the date the entity provides notice to consumers, whichever is sooner. Any entity that has, prior to the breach, sworn in writing on a form and in a manner prescribed by the Attorney General that the entity maintains written policies and procedures to maintain the security of personal information and respond to breaches in a manner consistent with state law shall notify the Attorney General before providing notice to consumers. Notice to the Attorney General shall contain the date the breach occurred, the date the breach was discovered, and a description of the breach. If the date of the breach is unknown, then the entity shall send notice to the attorney general as soon as the date becomes known. If an entity provides notice of the breach to consumers, the entity shall notify the Attorney General or the Department of the number of Vermont consumers affected, if known, and shall provide a copy of the notice that was provided to consumers. An entity may also send the Attorney General or Department a second copy of the notice to consumers that redacts the type of personal information breached for any public disclosure of the breach.
Notification of Credit Reporting Agencies	In the event an Entity is required to provide notice to more than 1,000 residents of Vermont at one time, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the department of banking, insurance, securities, and health care administration.
Notification by Third Parties	—
Timing of Notification	Notice of a breach must be made in the most expeditious time possible and without unreasonable delay, but no later than 45 days after discovery of the breach, consistent with the legitimate needs of law enforcement. The provision of notice may be delayed pending the completion of any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system, or at the request of a law enforcement agency if it believes notification would impede an investigation or jeopardize homeland or national security.

Form of Notification	Notice to affected individuals must be clear and conspicuous and include the following (if known to the data collector): • The incident in general terms • The type of personally identifiable information subject to breach • The general acts of the data collector to prevent further breach • A telephone number, toll-free if available, that the affected individual may call for further information and assistance • Advice directing the consumer to remain vigilant by reviewing account statements and free credit reports • Approximate date of breach A data collector may give notice by providing: • Written notice mailed to the consumer's residence • Electronic notice, where the data collector has a valid email address and subject to certain criteria • Substitute notice in certain circumstances Substitute notice will be appropriate if the covered entity demonstrates that the cost of providing notice will exceed $5,000 or that the class of affected individuals to be contacted by telephone or email exceeds 5,000 persons, or if the covered entity lacks sufficient contact information to provide notice to affected individuals, and consists of: • Conspicuous posting of the notice on the covered entity's website • Notification to major statewide and regional media
Exemptions or Safe Harbors	A financial institution that complies with the notification requirements of the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, or with the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice issued by the National Credit Union Administration is deemed to be in compliance with this statute.
Consequences of Non-Compliance	Vermont Attorney General and state's attorney have exclusive authority to investigate violations and enforce, prosecute, obtain, and impose remedies for a violation of this section.
Credit Monitoring Required	—

Virginia

State and Statute	Virginia CODE ANN. § 18.2-186.6
Covered Entities	The statute applies to any of the following entities that possess or license computerized data containing personal information: • Individuals, corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments and governmental subdivisions, agencies, or instrumentalities, or any other for-profit or non-profit legal entity
Definition of Personal Information	The first name or first initial and last name of an individual when combined with one or more of the following types of non-encrypted or non-redacted data relating to a Virginia resident: • Social Security number • Driver's license or state ID number • Debit or credit card account number, in combination with any security code, access code, or password that would permit access to a person's financial account • Passport number • Military identification number This category does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records available to the general public.
Definition of Breach	An unauthorized access and acquisition of unencrypted or non-redacted computerized data containing personal information, where such access and acquisition compromises the security or confidentiality of the personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals, and where the access and acquisition causes, or is reasonably believed to have caused, a resident of Virginia to become the victim of identity theft or other fraud. The definition of breach does not encompass good-faith acquisition of personal information by its owner or by an agent of its owner acting lawfully to acquire the individual's personal information.
Threshold for Notification	Where a covered entity discovers or is notified of a breach, and where the covered entity reasonably believes the breach has caused or will cause a resident of Virginia to become a victim of identity theft or fraud, the entity must disclose the breach. A covered entity must disclose a breach if encrypted information or an encryption key is accessed or acquired by an unauthorized individual in an unencrypted form.

Notification of Data Subject	Yes, and an entity that maintains computerized data that includes personal information that the entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the entity reasonably believes the personal information was accessed and acquired by an unauthorized person.
Notification of Government	Yes. The state Attorney General must be notified whenever any Virginia residents are notified under the criteria above. In the event an Entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, the state Attorney General of the timing, distribution, and content of the notice. For health information, the Entity must also notify the Commissioner of Health. Additionally, employers or payroll service providers that own or license computerized data relating to state income tax withheld must notify the Attorney General of unauthorized access and acquisition of unencrypted and unredacted computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person, and causes, or the employer or payroll provider reasonably believes has caused or will cause, identity theft or other fraud. For employers, the notification obligation applies only to information regarding its employees (not customers or other non-employees). Such employer or payroll service provider shall provide the Attorney General with the name and federal employer identification number of the employer without unreasonable delay after the discovery of the breach. The Attorney General shall then notify the Department of Taxation of the breach.
Notification of Credit Reporting Agencies	In the event an entity provides notice to more than 1,000 persons at one time pursuant to the general security breach section, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice.
Notification by Third Parties	—
Timing of Notification	Notice must be provided without unreasonable delay, but delay may be permissible when the covered entity needs to determine the scope of the breach and restore the integrity of the data system, or when a law enforcement agency advises the covered entity that notice would impede a criminal or civil investigation or jeopardize homeland or national security.

Form of Notification	Notice required by this section must include a description of: • The incident in general terms • The type of personal information subjected to unauthorized access and acquisition • The general steps taken by the covered entity to protect the personal information from further breach • A telephone number that the affected person may call for further information and assistance • Advice that directs the affected person to review account statements and monitor credit reports Notification may be effected by: • Written notice to the last known address in the records of the entity • Telephone notice • Electronic notice • Substitute notice, in certain circumstances Substitute notice will be appropriate if the individual or entity demonstrates that the cost of providing notice will exceed $50,000 or that the class of affected individuals exceeds 100,000 persons, or that the individual or entity lacks sufficient contact information to provide notice to affected individuals, and consists of all of the following: • Email notice if the individual or entity has email addresses for affected individuals • Conspicuous posting of the notice on the covered entity's website • Notification to major statewide media
Exemptions or Safe Harbors	Covered entities are deemed to be in compliance with this section if they are subject to Title V of the Gramm-Leach-Bliley Act and maintain procedures for notification of a breach in accordance with that Act and its applicable rules or regulations. A covered entity that complies with notification requirements established in the rules, regulations, or guidelines of its primary state or federal regulator is deemed to be in compliance with this section. A covered entity that maintains its own notification procedures as part of an information security policy is deemed to be in compliance with the notification requirements of the statute if the timing requirements are consistent with the statute and the entity provides notice in accordance with those policies in the event of a breach.

Consequences of Non-Compliance	Individuals have a private right of action to sue for damages and injunctions for violations of this statute. Attorney General of Virginia may impose civil penalties of up to $150,000 per breach or series of breaches. Enforcement by the covered entity's primary state regulator.
Credit Monitoring Required	—

Washington

State and Statute	Washington Rev. Code § 19.255.010 et seq.; § 42.56.590 Washington Rev. Code. § 42.56.590
Covered Entities	Any person or business that operates in the State of Washington and owns or licenses data containing personal information, or any person or business that does not own, but maintains data containing personal information.
Definition of Personal Information	(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: • Social Security number • Driver's license number or state identification card number • Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account, or [effective March 1, 2020] any other numbers or information that can be used to access a person's financial account [Additionally, effective March 1, 2020:] • Full date of birth • Private key that is unique to an individual and that is used to authenticate or sign an electronic record • Student, military, or passport identification number • Health insurance policy number or health insurance identification number • Any 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 • Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual (2) Username or email address in combination with a password or security questions and answers that would permit access to an online account; and (3) Any of the data elements or any combination of the data elements described in (1) above, without the consumer's first name or first initial and last name if: • Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and • The data element or combination of data elements would enable a person to commit identity theft against a consumer. PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Definition of Breach	An unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information. The definition of breach does not encompass good-faith acquisition of personal information by the individual or by an agent of the individual acting lawfully to acquire the individual's personal information.
Threshold for Notification	Covered entity must notify affected individuals if it knows or reasonably believes that an individual's personal information was acquired by an unauthorized person. This provision does not apply to technical breaches of security that do not seem reasonably likely to subject customers to a risk of harm.
Notification of Data Subject	Yes, and any entity that maintains computerized data that includes personal information that the entity does not own shall notify the owner or licensee of the information of any breach immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Government	Yes.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	—
Timing of Notification	The disclosure to affected consumers and to the Attorney General shall be made in the most expeditious time possible and without unreasonable delay, no more than 30 [45, effective March 1, 2020] calendar days after the breach was discovered, unless the delay is at the request of law enforcement or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Form of Notification	Notification of the breach must be provided by one of the following methods: • Written notice • Electronic notice if consistent with the requirements of 15 U.S.C. § 7001 • Substitute notice, in certain circumstances The notification must be written in plain language and must include, at a minimum, the following information: • The name and contact information of the reporting person or business subject to this section • A list of the types of PI that were or are reasonably believed to have been the subject of a breach • [Effective March 1, 2020] A timeframe of exposure, if known, including the date of the breach and the date of the discovery of the breach • The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed PI Substitute notice will be appropriate if the individual or entity demonstrates that the cost of providing notice will exceed $250,000 or that the class of affected individuals exceeds 500,000 persons, or that the individual or entity lacks sufficient contact information to provide notice to affected individuals, and consists of: • Email notice if the individual or entity has email addresses for affected individuals; • Conspicuous posting of the notice on the entity's website; and • Notification to major statewide media; or [Effective March 1, 2020] If the breach of the security of the system involves personal information, including a username or password, notice may be provided electronically or by email. If the breach involves login credentials of an email account furnished by the Entity, notice may be provided using another method; not to that email address. The notice must inform the individual whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the Entity and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer.

Exemptions or Safe Harbors	Processors, businesses, and vendors are not liable if the personal information was encrypted at the time of the breach, or if the processor, business, or vendor was certified "compliant" with the payment card industry data security standards in force at the time of the breach, if compliance was validated by an annual security assessment within one year prior to the breach. A person or business that maintains its own notification procedures as part of an information security policy is deemed to be in compliance with the notification requirements of the statute if the timing requirements are consistent with the statute and the entity provides notice in accordance with those policies.
Consequences of Non-Compliance	Individuals have a private right of action to sue for damages and injunctions for violations of this statute. The rights and remedies of this statute are cumulative to each other and to any other rights and remedies under law.
Credit Monitoring Required	—

West Virginia

State and Statute	West Virginia CODE §§ 46A-2A-101 et seq.
Covered Entities	Any of the following entities that own or license personal information: • Corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnership, limited liability companies, associations, organizations, joint ventures, governments or governmental subdivisions, agencies, or instrumentalities, and any other for-profit or non-profit legal entity
Definition of Personal Information	The first name or first initial and last name of an individual when combined with one or more of the following types of non-redacted or unencrypted data: • Social Security number • Driver's license or state ID number • Debit or credit card account number, in combination with any security or access code, or password that would permit access to a person's financial account The term does not include information that is lawfully obtained from publicly available information, or from federal, state or government records available to the general public.
Definition of Breach	An unauthorized acquisition of unencrypted and non-redacted computerized data that compromises the personal information of an individual, or that causes an individual or entity to reasonably believe that the breach has caused or will cause a resident of West Virginia to become a victim of identity theft or fraud. The definition of breach does not encompass a good-faith acquisition of personal information by the individual or an agent of the individual seeking to acquire personal information lawfully.
Threshold for Notification	Covered entity must provide notice to affected individuals if it knows or reasonably believes that the breach will cause a resident of West Virginia to become the victim of identity theft or fraud.
Notification of Data Subject	Yes, and an entity that maintains computerized data that includes personal information that the entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or the entity reasonably believes was accessed and acquired by an unauthorized person.
Notification of Government	If an entity is required to notify more than 1,000 persons of a breach of security pursuant to this article, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis of the timing, distribution, and content of the notices.

Notification of Credit Reporting Agencies	Nothing in this subsection shall be construed to require the entity to provide to the consumer reporting agency the names or other personal information of breach notice recipients.
Notification by Third Parties	—
Timing of Notification	The entity must provide notice without unreasonable delay and as soon as practicable following discovery. Delay may be appropriate where a law enforcement agency advises the covered entity that notice will impede a criminal investigation, or where the entity must take measures necessary to determine the scope of the breach or restore the integrity of the security system protecting the personal information.
Form of Notification	Notification of the breach, including a description of the information most likely to have been acquired, must include: • A telephone number or internet address that an individual may use to contact the entity or its agency to determine the scope of the entity's breach and the risk to the individual's personal information • A toll-free number for the major credit reporting agencies and information on how to place a security freeze on an account Notification may be effected by: • Written notice • Telephone notice • Electronic notice, if consistent with 15 U.S.C. § 7001 • Substitute notice, in certain circumstances Substitute notice will be appropriate if the individual or entity demonstrates that the cost of providing notice will exceed $50,000 or that the class of affected individuals exceeds 100,000 persons, or that the individual or entity lacks sufficient contact information to provide notice to affected individuals, and consists of any two of the following: • Email notice if the individual or entity has email addresses for affected individuals • Conspicuous posting of the notice on the entity's website • Notice to major statewide media

Exemptions or Safe Harbors	The statute does not apply to information that is encrypted or redacted, as long as the encryption key was not accessed by unauthorized individuals. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system. The notification provisions do not apply to an entity subject to Title V of the Gramm Leach Bliley Act, 15 U.S.C. § 6801 et seq.
Consequences of Non-Compliance	State Attorney General may enforce civil penalties. If the violations of this statute are repeated and willful, penalties up to $150,000 are permissible. No private right of action.
Credit Monitoring Required	—

Wisconsin

State and Statute	Wisconsin STAT. § 134.98
Covered Entities	A person, other than an individual, that: • Conducts business in Wisconsin and maintains personal information in the course of business • Licenses personal information in Wisconsin • Maintains a depository account for a Wisconsin resident • Lends money to a Wisconsin resident This statute covers: • The State of Wisconsin and any of its offices • Independent agencies • Authorities, institutions, associations, societies, or other bodies of state government including the state legislature and courts • Wisconsin cities, villages, towns, and counties
Definition of Personal Information	The first name or first initial and last name of an individual when combined with one or more of the following types of non-redacted, non-public, or unencrypted data: • Social Security number • Driver's license or state ID number • Debit or credit card account number, in combination with any security or access code, or password that would permit access to a person's financial account • DNA profile – the individual's deoxyribonucleic acid profile • Unique biometric data including fingerprints, voiceprints, retina or iris images, or any other unique physical representation
Definition of Breach	Breach: an unauthorized acquisition of personal information by an unauthorized person, including where a person who does not own or license personal information knows that the information has been acquired by an unauthorized individual and has not entered into a contract with an individual who owns or licenses the personal information.

Threshold for Notification	If an entity conducting business in the state, or whose principal place of business is located in the state, knows that personal information in their possession has been acquired by an unauthorized individual, the entity shall make reasonable efforts to notify the affected individuals. If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. Notification is not required where: • The breach does not create a material risk of identity theft or fraud to the affected individual • The personal information was acquired in good faith by an employee or agent of an individual for a lawful purpose
Notification of Data Subject	Yes, and if a person, other than an individual, that stores personal information pertaining to a resident of Wisconsin, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has been not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the personal information shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable.
Notification of Government	—
Notification of Credit Reporting Agencies	If, as the result of a single incident, an entity is required to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices sent to the individuals.
Notification by Third Parties	—
Timing of Notification	The entity must provide notice within a reasonable time, and as soon as practicable following determination of a breach, not to exceed 45 days after discovery of the breach. Notification may be delayed consistent with the legitimate needs of a law enforcement agency when conducting an investigation or protecting homeland security.

Form of Notification	Notification must be provided by one of the following: • Mail • Other means used to communicate with the affected person If, after reasonable diligence, the mailing address of the affected individual cannot be discovered and the entity has not communicated with the affected individual about the data breach, the entity must provide notice in a method reasonably calculated to provide actual notice to the affected individual.
Exemptions or Safe Harbors	Notification is not required if the acquisition of the personal information does not create a material risk of identity theft or fraud to the affected individual.
Consequences of Non-Compliance	Violation of the statute may be evidence of negligence or breach of a legal duty in a legal proceeding.
Credit Monitoring Required	—

Wyoming

State and Statute	Wyoming STAT. ANN. § 40-12-501 et seq.
Covered Entities	Any individual or commercial organization that conducts business in Wyoming that owns, licenses, or maintains computerized data containing personal identifying information about a Wyoming resident.
Definition of Personal Information	The first name or first initial and last name of an individual when combined with one or more of the following types of non-redacted data: • Social Security number • Driver's license or state ID number • Debit or credit card account number, in combination with any security or access code, or password that would permit access to a person's financial account • Tribal identification card • Identification documents issued by the federal or state government
Definition of Breach	An unauthorized acquisition of data that materially compromises the security, confidentiality, or integrity of personal identifying information that causes or is reasonably believed to have caused loss or injury. Good-faith acquisition of such data by a person or organization acting on behalf of the owner of the personal identifying information does not qualify as a breach.
Threshold for Notification	After conducting a reasonable and prompt investigation, if the person or organization determines that the personal identifying information has been or is reasonably likely to be misused, the person or organization must disclose the breach.
Notification of Data Subject	Yes, and an Entity that maintains computerized data that includes personal information on behalf of another Entity shall disclose to the Entity for which the information is maintained any breach of the security of the system as soon as practicable following the determination that personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The Entity that maintains the data on behalf of another Entity and Entity on whose behalf the data is maintained may agree which Entity will provide any required notice, provided only a single notice for each breach of the security of the system shall be required. If agreement regarding notification cannot be reached, the Entity who has the direct business relationship with the resident of WY shall provide the required notice.
Notification of Government	No.
Notification of Credit Reporting Agencies	—

Notification by Third Parties	—
Timing of Notification	The individual or organization must provide notice to affected residents in the most expeditious fashion possible and without unreasonable delay. Notification may be delayed consistent with the legitimate needs of a law enforcement agency (provided in writing) or with any measures necessary to determine the scope of the breach and restore the integrity of the computerized system.
Form of Notification	Notification must include, at minimum: • A toll-free number that individuals may use to contact the entity collecting the data and from which individuals can learn the toll-free phone numbers for the major credit reporting agencies • The types of personal information that were or are reasonably believed to have been the subject of the breach • A general description of the breach incident • The approximate date of the breach, if that information is reasonably available • The actions taken to protect the system from further breaches • Advice to remain vigilant in reviewing account statements and credit reports • Whether notification was delayed due to law enforcement investigations if that information is reasonably possible to determine at the time notice is provided. Notification may be made by: • Written notice • Electronic notice • Substitute notice, in certain circumstances Substitute notice is appropriate where: • The cost of providing Wyoming residents or businesses would exceed $10,000 and providing notice to out-of-state businesses would exceed $250,000 • Number of affected Wyoming-based individuals or businesses exceeds 10,000, or the number of affected businesses operating in Wyoming exceeds 500,000 • The possessor or licensor of the personal information does not have sufficient contact information for affected individuals Substitute notice may consist of any of the following: • Conspicuous posting on the website of the individual or business experiencing the breach, including a toll-free number for the breached entity and the major credit reporting agencies • Notification to major statewide media outlets, including a toll-free number for affected individuals to determine the status of their personal identifying information

Exemptions or Safe Harbors	Any financial institution as defined in 15 U.S.C. § 6809 or federal credit union as defined by 12 U.S.C. § 1752 is deemed to be in compliance with the statute if the institution notifies Wyoming customers in compliance with 15 U.S.C. § 6801 et seq. and applicable agency regulations.
Consequences of Non-Compliance	State Attorney General may bring an action in law or in equity, or for any other relief that may be appropriate to address any violation of this statute.
Credit Monitoring Required	—

omm.com