O'Melveny

A Guide to US Breach Notification Laws

The ever-increasing importance of technology-driven solutions to daily operations, and both state and federal regulators' growing focus on organization-level security procedures, require a rapid response from companies when confronted with a cybersecurity threat.

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 as company executives and in positions at various levels of government, including:

- Former Deputy Associate Director, Financial Crimes Enforcement Network of the US Department of the Treasury
- Former Cyber Hacking and Intellectual Property Attorney, Digital Currency Crimes Coordinator, and the sole National Security Cyber Specialist
- Former Assistant US Attorney in the Northern District of Texas's National Security, Cybercrime and Money Laundering Division
- Former Data Privacy Officer, alternative coin and blockchain company
- Former General Counsel, major media company

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

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

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

Sid Mody
Partner
Dallas
+1 945 221 1645
smody@omm.com

CONTENTS BY STATE AND TERRITORY

Alabama 1
Alaska 5
Arizona 8
Arkansas 12
California 15
Colorado 20
Connecticut 24
Delaware 28
District of Columbia 32
Florida 36
Georgia 40
Guam 43
Hawaii 46
Idaho 50
Illinois 53
Indiana 57
Iowa 61
Kansas 65
Kentucky 68
Louisiana 71
Maine 75
Maryland 79
Massachusetts 84
Michigan 88
Minnesota 92
Mississippi 95
Missouri 98
Montana 102
Nebraska 105
Nevada 108
New Hampshire 111
New Jersey 115
New Mexico 119
New York 123
North Carolina 127
North Dakota 131
Ohio 134
Oklahoma 138
Oregon 141
Pennsylvania 146
Puerto Rico 150
Rhode Island 153
South Carolina 157
South Dakota 160
Tennessee 163
Texas 166
US Virgin Islands 169
Utah 172
Vermont 175
Virginia 180
Washington 184
West Virginia 188
Wisconsin 191
Wyoming 194

CONTENTS BY TOPIC

State and Statute

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

Covered Entities

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

Definition of Personal Information

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

Definition of Breach

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

CONTENTS BY TOPIC

Threshold for Notification

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

Notification of Data Subject

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

Notification of Government

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

Notification of Credit Reporting Agencies

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

CONTENTS BY TOPIC

Notification by Third Parties

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

Timing of Notification

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

Form of Notification

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

Exemptions or Safe Harbors

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

CONTENTS BY TOPIC

Consequences of Non-Compliance

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

Credit Monitoring Required

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

ALABAMA

State and Statute	Alabama Code § 8-38-1 et seq.
Covered Entities	Persons, sole proprietorships, partnerships, government entities, corporations, nonprofits, trusts, estates, cooperative associations, or other business entities that acquire or use sensitive personally identifying information.
Definition of Personal Information	Information containing an Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident: • Social Security number • Tax identification number • Driver's license number • State-issued identification card number • Passport number • Military identification number • Other unique identification number issued on government document to verify individual's identity • Financial account number, including bank account number, credit card number, debit card number, in combination with any security code, access code, password, expiration date, or PIN that is necessary to access the financial account or conduct a transaction • Any information regarding the individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional • Health insurance policy number, subscriber identification number, and any unique identifier used by a health insurer to identify an individual • 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).

ALABAMA

	• 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 a covered entity is not a security breach, unless the information is 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
Threshold for Notification	After the covered entity, that is not a third-party agent, determines that a breach of security has or may have occurred in relation to sensitive personally identifying information that is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the covered entity and 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 the individuals to whom the information relates.
Notification of Government	Yes, if the number of affected individuals exceeds 1,000, the entity must provide written notice of the breach to 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.

ALABAMA

Notification of Credit Reporting Agencies	Yes, consumer reporting agencies must be informed without unreasonable delay if the breach exceeds 1,000 individuals at a single time and is likely to cause substantial harm to the affected individuals.
Notification by Third Parties	Yes, an entity that has been contracted to maintain, store, process, or is otherwise permitted to access sensitive personally identifying information in connection with providing services to a covered entity ("Third Party Agent") that has experienced a breach of security in the system maintained by the agent shall notify the covered entity of the breach of security as expeditiously as possible and without unreasonable delay, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred.
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) actions taken by the covered entity in response to the breach, 4) steps individual can take to protect themselves, and 5) information the individual can use to contact the covered entity about the breach. *Exception:* 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:*

ALABAMA

	Publication on company website for 30 days (in a conspicuous location) and notice to major print and broadcast media in the affected area. Alternative form of substitute notice may be used with the approval of the attorney general.
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. There is also a safe harbor for encrypted information.
Consequences of Non-Compliance	*Government enforcement?* A violation of the notification provisions 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 will be subject to the penalty provisions of the statute. A covered entity that violates the notification provisions 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, there is no private right of action.
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 Alaska that includes personal information of an Alaska resident.
Definition of Personal Information	Information containing an individual's first name or first initial and last name in combination with one or more of the following: • Social Security number • Driver's license number • State identification card number • Credit card, debit card, and/or bank account number • Information necessary to access financial accounts (including but not limited to passwords, PIN numbers, and access codes) *Exception:* 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 maintained by the information collector. Acquisition includes acquisitions 1) by photocopying, facsimile, or other paper-based method, 2) by a device that can read, write, or store information represented in numerical form (including a computer), or 3) any other method. *Exception:* Good-faith acquisition of personal information by an employee or agent of the information collector for a legitimate purpose.
Threshold for Notification	When the breach is likely to cause "reasonable" harm to the residents of the state whose personal information was compromised.

ALASKA

Notification of Data Subject	Yes, any entity to which the statute applies must disclose the breach to each Alaska resident whose personal information was subject to the breach after discovering or being notified of the breach. *Exception*: 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 (5) years.
Notification of Government	No, covered entities are not required to report a security breach to the state attorney general or other government agency.
Notification of Credit Reporting Agencies	Yes, credit reporting agency must be notified if more than 1,000 residents of the state must receive notification. Names or other personal information of the Alaska residents affected by the breach are not required to be provided. *Exception*: Entities subject to the Gramm-Leach-Bliley Act are exempt from this requirement.
Notification by Third Parties	Yes, third party must notify covered entity who owns or licenses the personal information at issue. Third party must provide notice immediately after discovering the breach and cooperate with covered entity so that it is able to comply with the notice requirement.
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 provide a substitute notice 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 *Substitute notice:* • 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	Judicial agencies and persons with less than ten employees. Safe harbor exists for encrypted information.
Consequences of Non-Compliance	*Government enforcement?* If an information collector is not a government agency, the violation is an unfair or deceptive act or practice. The information collector may be liable to the state for up to $500 for each state resident who was not notified. Total civil penalty may not exceed $50,000. *Private right of action?* Yes, there is a private right of action under the unfair competition/deceptive practice portion of the statute. The affected individual may bring a civil action to recover for each unlawful act or practice, three times the actual damages or $500, whichever is greater (which applies to both individual and class actions). Damages that may be awarded under attorney fees, costs, and damages are limited to actual economic damages.
Credit Monitoring Required	—

ARIZONA

State and Statute	Arizona Rev. Stat. § 18-551 et seq.
Covered Entities	A natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity that conducts business in Arizona and owns, maintains or licenses unencrypted and unredacted computerized personal information.
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 • Arizona driver's license number or nonoperating identification license number • Credit card, debit card, and/or financial account number in combination with any required security code, access code, or password to access the account • Health insurance identification number • Any information regarding the individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional • Passport number • Taxpayer identification number or identity protection personal identification number issued by the IRS • Unique biometric data for body characteristics *Exception:* Any information about an individual made public by the federal, state, and/or local government.
Definition of Breach	An unauthorized acquisition of and unauthorized access that materially "compromises the security or confidentiality" of unencrypted and unredacted computerized personal information maintained as a part of a database of personal information regarding multiple individuals. *Exception:* If the personal information was retrieved in good faith by the employee or agent of the person and it was not used for a purpose unrelated to the person or subject to further unauthorized disclosure.

ARIZONA

Threshold for Notification	When the covered entity discovers unauthorized and unreasonable retrieval of computerized, unencrypted data, and the covered entity conducts a "reasonable investigation" through an independent third-party auditor or law enforcement agency and determines that there has been a breach.
Notification of Data Subject	Yes, any entity that owns or licenses the affected personal information shall notify the affected individuals within 45 days after determination that there has been a security breach. *Exception:* 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 individuals.
Notification of Government	Yes, if the breach exceeds 1,000 individuals, the attorney general and the director of the Arizona Department of Homeland Security must be notified in writing or with a copy of the notification, within 45 days after the determination of a breach.
Notification of Credit Reporting Agencies	Yes, if the breach exceeds 1,000 individuals, consumer reporting agencies must be notified, within 45 days after determination of the breach.
Notification by Third Parties	Yes, a person that maintains unencrypted and unredacted computerized personal information that the person does not own or license shall notify, as soon as practicable, the owner or licensee of the information on discovering any security system breach and cooperate with the owner or the licensee of the personal information, including sharing information relevant to the breach with the owner or licensee.
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.

ARIZONA

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 provide a substitute notice 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:* Written letter to attorney general that demonstrates the facts necessary and conspicuous posting of notice on company website for at least 45 days, if available.
Exemptions or Safe Harbors	There is a safe harbor for encrypted information that uses a "process to transform data into a form that renders the data unreadable or unusable without using a confidential process or key." *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. *Exempt entities:* • HIPAA-covered entities • Person subject to Title IV of the Gramm-Leach-Bliley Act of 1999
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 the lesser of (i) $10,000 per breach and (ii) the total amount of economic loss sustained by affected individuals. The

	maximum civil penalty may not exceed $500,000. Covered entities must “willfull[y]” and “knowing[ly]” violate notification procedures to be liable. *Private right of action?* No, there is no private right of action.
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 computerized data that includes personal information. Businesses include entities "that destroy records" and state agencies.
Definition of Personal Information	Information containing an individual's first name or first initial and last name and one or more of the following, when either the name or data element is not encrypted or redacted: • Social Security number • Driver's license number or Arkansas identification card 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 a person or business. *Exception:* Good-faith acquisition of personal information.
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.

ARKANSAS

Notification of Data Subject	Yes, notice must be given to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, and where there is a reasonable likelihood of harm to customers.
Notification of Government	Yes, the attorney general must be notified 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. An entity must retain a copy of the determination of the breach and any supporting documentation for five (5) years from the date the breach was determined.
Notification of Credit Reporting Agencies	No, notice to credit reporting agencies is not required.
Notification by Third Parties	Yes, any person or business that maintains computerized data that includes personal information that person or business does not own must 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.
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 provide a substitute notice if one or more of the following situations occurs: • The cost of providing notice exceeds $250,000 • The number of affected individuals exceeds 500,000 persons

	• Contact information for affected individuals is unavailable *Substitute notice:* • Email to the persons affected, if available • Conspicuous posting of notice on company website, if available • Notice in statewide media
Exemptions or Safe Harbors	There is a safe harbor for encrypted information. *Following entity's own notification procedures?* Yes, a person or business will be deemed to be in compliance 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, a person or business will be deemed to be in compliance 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. Remedies concerning deceptive trade practices include restitution, injunctive relief, and civil penalties up to $10,000 per violation. Violation may also be subject to suspension or forfeiture of franchises, corporate charters, or other licenses, permits, or authorization to do business in Arkansas. Knowing and willful violation of the statute concerning deceptive trade practices is a Class A misdemeanor. *Private right of action?* No, there is no private right of action.
Credit Monitoring Required	—

CALIFORNIA

State and Statute	California Civ. Code § 1798.29 (agencies) California Civ. Code § 1798.80 (businesses) California Health and Safety Code § 1280.15 California Consumer Privacy Act (as amended by the California Privacy Rights Act) (collectively, the "CCPA")
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. Medical clinics health facilities, hospitals and home health facilities (California Health and Safety Code § 1280.15).
Definition of Personal Information	(1) Information containing an individual's name and one or more of the following (with respect to a California resident): • A Social Security number • A driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual • An 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 • Medical information • Health insurance information • Unique biometric data • Information or data collected through the use or operation of an automated license plate recognition system • Genetic data (2) A username or email address, in combination with a password or security question and answer that would permit access to an online account.

	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. *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 by an agent of the business for the purpose of the business as long as the information is not subject to further unauthorized disclosure.
Threshold for Notification	When a covered entity discovers or has reason to believe that unencrypted personal information has been retrieved by an unauthorized individual. California's Office of Privacy Protection also 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, notice of a breach must be given to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Government	Yes, if an entity is required to notify more than 500 California residents, the entity shall electronically submit a single sample copy of the notification, excluding any personally identifiable information, to the California Attorney General.
Notification of Credit Reporting Agencies	—

CALIFORNIA

Notification by Third Parties	Yes, a person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the 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.
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.
Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written or electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001) Substitute notification is available if the cost of providing notice would exceed $250,000, the number of people affected exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notification must consist of all of the following: • Email notice when the person or business has an email address for the subject persons • Conspicuous posting, for a minimum of 30 days, of the notice on the internet website page of the person or business, if the person or business maintains one • Notification to major statewide media
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. A limited safe harbor for encrypted information that applies when either (1) the encryption key or security credential was not, or is reasonably believed to not have been, acquired by an unauthorized person, or (2) the person or business that owns or licenses the encrypted information reasonably believes that the encryption key or security credential could not render that personal information readable or usable.
Consequences of Non-Compliance	*Government enforcement?* No, the general breach notification statute does not specifically provide for regulatory enforcement. The California Department of Health Services may issue a penalty of up to $25,000 per patient whose medical information was unlawfully or without authorization accessed, used, or disclosed, and up to $17,500 per subsequent occurrence of unlawful or unauthorized access, use or disclosure of the patient's medical information. For covered entities who fail to report a breach: • 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 *Private right of action?* Yes, private individuals injured by an entity's failure to follow notification procedures may "recover damages" and seek injunctive relief. See § 1798.84(b). **California Consumer Privacy Act of 2018** Any consumer whose nonencrypted and nonredacted personal information or whose email address in combination with a password or security questions and answers that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure 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 Actions pursuant to this statute 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 the statute 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 statute. • If a business continues to violate this statute in breach of the express written statement provided to the consumer under this statute, 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.
Credit Monitoring Required	Credit Monitoring Required for 12 months if breach included SSN.

COLORADO

State and Statute	Colorado Rev. Stat. § 6-1-716 (Pg. 68)
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.
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 email 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. *Exception:* 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	When it becomes aware that a security breach may have occurred, covered entity must conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. Notice must be given as soon as possible to the Colorado resident, unless the investigation determines the misuse of information has not occurred and is not reasonably likely to occur.
Notification of Data Subject	Yes, covered entities must provide notice of a breach to affected Colorado residents.
Notification of Government	Yes, if breach is reasonably believed to have affected more than 500 Colorado residents, the covered 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	Yes, if there are more than 1,000 affected Colorado residents, credit reporting agencies must be notified of "the anticipated date of the notification to the residents and the approximate number of residents who are to be notified" in the most expedient time possible and without unreasonable delay. *Exception*: Covered entities subject to Title V of the federal Gramm-Leach-Bliley Act are not required to notify credit reporting agencies.
Notification by Third Parties	Yes, if a covered entity uses a third-party service provider to maintain computerized data, including personal information, then the third-party service provider must notify covered entity of any security breach in the most expedient time possible and without unreasonable delay.
Timing of Notification	Notice must be made in the most expeditious time possible and without unreasonable delay, but no later than 30 days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

COLORADO

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 provide a substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $250,000 • The number of affected Colorado residents exceeds 250,000 • Contact information for affected individuals is unavailable *Substitute notice*: • Email the affected person if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notification to major statewide media
Exemptions or Safe Harbors	There is a safe harbor for encrypted information "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security." *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 or functional state or federal 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 [statute] or recover direct economic damages resulting from a violation, or both."

	Upon receipt of notice and either a request from the governor or with the approval of the district attorney with jurisdiction to prosecute, the attorney general also has the authority to prosecute any criminal violations. *Private right of action?* No, there is no express private right of action.
Credit Monitoring Required	—

CONNECTICUT

State and Statute	Connecticut Gen. Stat. § 36a-701b
Covered Entities	Any person who owns, licenses or maintains computerized data that includes personal information.
Definition of Personal Information	Information containing an individual's first name or first initial and last name in combination with one or more of the following: • Social Security number • Taxpayer identification number • Identity protection personal identification number issued by IRS • Driver's license number, state identification number, passport number, military identification number, or other government-issued 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) • Medical information regarding medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional • Health insurance policy number, subscriber identification number, or any unique identifier used by health insurer • Biometric information consisting of data generated by an individual's unique physical characteristics (finger print, voice print, retina, iris image) • Precise geolocation data *Exception:* 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.

CONNECTICUT

Threshold for Notification	When the breach is likely to cause reasonable harm to the residents of the state whose personal information was compromised. *Exception*: An investigation is conducted with relevant federal, state, and local law enforcement agency and it is reasonably determined that "the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."
Notification of Data Subject	Yes, covered entity shall disclose any breach of security following the discovery of the breach to any Connecticut resident whose personal information was breached, or is reasonably believed to have been breached and such breach will likely result in harm to the individual.
Notification of Government	Yes, to Connecticut's attorney general; notice must be provided no later than it is provided to the affected residents.
Notification of Credit Reporting Agencies	No, notification to credit reporting agency is not required.
Notification by Third Parties	Yes, any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information of a resident of this state was breached or is reasonably believed to have been breached.
Timing of Notification	Notifications must be sent "without unreasonable delay," but no later than 60 days after discovery of the breach, unless federal law requires a shorter time. *Exception:* 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.

CONNECTICUT

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 substitute notice if one or more of the following situations occurs: • The cost of notifying the affected class exceeds $250,000 • The number of affected individuals exceeds 500,000 • Contact information for affected individuals is unavailable *Substitute notice:* • Email the affected person 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	There is a safe harbor for encrypted information. *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 or functional regulator. If notice is given to a Connecticut 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 statute 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, there is no express private right of action.

CONNECTICUT

Credit Monitoring Required	Credit monitoring required for 24 months if breach included: (i) Social Security number; or (ii) taxpayer identification number.

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 Delaware 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 *Exception*: 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. *Exceptions:* • 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. • 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 a Delaware resident's personal information was breached or is reasonably believed to have been breached. *Exception*: An investigation is conducted, and it is reasonably determined that the breach will not likely result in harm to the individuals whose personal information has been breached.
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 Delaware 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.

DELAWARE

Notification of Credit Reporting Agencies	No, notice of breach to credit reporting agencies is not required.
Notification by Third Parties	Yes, third parties must give notice if covered entity maintains covered information on behalf of other entity immediately following discovery of the breach.
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 provide a substitute notice if one or more of the following situations occurs: • The cost of notifying the affected class exceeds $75,000 • The number of affected Delaware residents exceeds 100,000

	• Contact information for affected individuals is unavailable *Substitute notice:* • Email the affected individuals if email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	There is a safe harbor for encrypted information, which is "personal information that is rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security." *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 or functional state or federal regulator.
Consequences of Non-Compliance	*Government enforcement?* Yes, at the attorney general's discretion. *Private right of action?* No, there is no private right of action.
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 the District of Columbia and own or license personal information about District of Columbia residents in the form of computerized "or other electronic" data.
Definition of Personal Information	Information consisting of an individual's first name, first initial and last name, or any other personal identifier, which can be used to identify a person or the person's information when combined with any of the following: • Social Security number • Individual tax identification number • Passport number • Driver's license number or other DC identification number • Military 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) • Medical information • Genetic information and deoxyribonucleic acid (DNA) profile • Health insurance information, including policy number, subscriber information number, or any unique identifier used by health insurer • Biometric data of an individual, such as fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic used to uniquely authenticate the individual's identity Personal information also includes (1) any combination of the above-mentioned data elements that would enable a person to commit identity theft without reference to a person's first name or first initial and last name or other independent personal identifier, and (2) a user name or e-mail address in combination with a password, security question and answer, or other means of authentication, or any combination of data elements included in the bullets above that permits access to an individual's email account. *Exception:*

DISTRICT OF COLUMBIA

	Any information about an individual made public by the federal, state, and/or local government.
Definition of Breach	An unauthorized acquisition of "computerized or other electronic data, or any equipment or device storing such data" that "compromises the security, confidentiality, or integrity" of personal information maintained by the person or entity who conducts business in DC. *Exceptions:* • A good-faith acquisition of personal information that is not used improperly or subject to further unauthorized disclosure • Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party • Acquisition of personal information the person or entity reasonably determines, after a reasonable investigation and consultation with the attorney general and federal law enforcement agencies, will likely not result in harm to the individual.
Threshold for Notification	When the covered entity discovers any breach of the security of the system.
Notification of Data Subject	Yes, any entity to which the statute applies, and who discovers a breach of the security system, shall promptly "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement" notify any District of Columbia resident whose personal information was included in the breach.
Notification of Government	Yes, any entity required to give notice to District of Columbia residents must also promptly provide written notice to the Office of Attorney General if the breach affects 50 or more District of Columbia residents. The notice shall be made in the most expedient manner, no later than when notice is provided to District of Columbia residents. It cannot be delayed on grounds that the total number of affected District of Columbia residents has not yet been ascertained.
Notification of Credit Reporting Agencies	Yes, credit reporting agency reporting required so long as personal information for more than 1,000 District of Columbia 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.

DISTRICT OF COLUMBIA

Notification by Third Parties	Yes, any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery.
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 a covered entity may delay notification until disclosure will not disrupt the investigation.
Form of Notification	The notice must describe: (1) a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, (2) contact information for the person or entity making the notification, (3) the toll-free telephone numbers and addresses for major consumer reporting agencies, and (4) the toll-free numbers, addresses and website addresses for the FTC and Office of the Attorney General for the District of Columbia. 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 provide a substitute notice if one or more of the following situations occurs: • The cost of notifying the affected class exceeds $50,000 • The number of affected individuals exceeds 100,000 • Contact information for affected individuals is unavailable *Substitute notice:* • Email the affected individuals if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify local and national media, if applicable

DISTRICT OF COLUMBIA

Exemptions or Safe Harbors	There is safe harbor for encrypted information that has been rendered secure so as to be unusable by a third party. *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 or the U.S. Department of Health and Human Services pursuant to HITECH, it shall be deemed to be in compliance.
Consequences of Non-Compliance	*Government enforcement?* Yes, any violation of DC's data breach notification statute is considered an unfair or deceptive trade practice, which may be investigated by the Department of Licensing and Consumer Protection. *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.
Definition of Personal Information	Information containing an individual's first name or first initial and last name in combination with one or more of the following: • Social Security number • Driver's license number • Identification card number • Passport number • Military identification number • Similar identification number on a government-issued document • 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, mental or physical condition, and/or prior diagnoses • Information used by health insurer to identify the individual, such as a policy number or subscription identification number • A username or email address in combination with a password or security question and answer that would permit access to an online account *Exception:* 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. *Exception:* 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	When the covered entity "reasonably believes" that the personal information of any Florida resident was accessed as a result of the breach and there is a risk of financial harm to the individual whose personal information was accessed. *Exception:* 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 attorney general through 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 within 30 days of the breach. 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: • Summary of the facts surrounding the breach • The number of Florida residents affected or potentially affected by the breach • An overview of the services that the covered entities offer affected residents with instructions sent to individuals as to how to use such services • 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."

FLORIDA

Notification of Credit Reporting Agencies	Yes, 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	Yes, in the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred.
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	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 covered entity may provide substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $250,000 • The number of affected individuals exceeds 500,000 • Contact information for affected individuals is unavailable *Substitute notice:* • 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

FLORIDA

Exemptions or Safe Harbors	There is a safe harbor for encrypted information. *Following agency's guidelines?* Yes, so long as the covered entity follows procedures set forth by its primary or functional federal regulator.
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 may 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, there is no private right of action.
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. *Exception:* 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	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

GEORGIA

	Exception: 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. *Exception:* 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 Georgia whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Government	No, notice to government agency is not required.
Notification of Credit Reporting Agencies	Yes, if personal information for more than 10,000 Georgia residents has been breached at a single time.
Notification by Third Parties	Yes, third parties that maintain computerized data, including personal information they do not own, must notify information broker or data collector of any breach within 24 hours of discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.
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 a covered entity may delay notification until disclosure will not disrupt the investigation.

GEORGIA

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 covered entity may provide substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $50,000 • The number of affected individuals exceeds 100,000 • Contact information for affected individuals is unavailable *Substitute notice:* • Email the affected individuals if their email address is available • Conspicuous disclosure of information on the covered entity's website, if available • Notice to major statewide media
Exemptions or Safe Harbors	There is a safe harbor for encrypted information. *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?* No, the data breach notification statute does not specify penalties for violation. *Private right of action?* No, there is no express private right of action.
Credit Monitoring Required	—

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 Guam 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) *Exception:* 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 personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of Guam. *Exception*: 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	When the covered entity discovers or is notified of 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.

GUAM

Notification of Government	—
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Yes, third parties that maintain computerized data that includes personal information that the individual or entity does not own or license shall notify 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 if the entity reasonably believes was, accessed and acquired by an unauthorized person.
Timing of Notification	Notifications must be sent without unreasonable delay. *Exception*: 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 provide substitute notice if one or more of the following situations occurs: • The cost of notifying persons exceeds $10,000 • The number of affected individuals exceeds 5,000 • Contact information or consent for affected individuals is unavailable *Substitute notification, any two of the following:* • Email the affected individuals if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notice to major Guam media

GUAM

Exemptions or Safe Harbors	*Following entity's own notification procedures?* Yes, 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 shall be deemed to be in compliance if it notifies residents of Guam in accordance with its procedures. *Following agency's guidelines?* Yes, for financial institutions, so long as the financial institution follows procedures set forth by its primary or functional federal regulator. 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	*Government enforcement?* Yes, violations may result in actual damages or civil penalties not exceeding $150,000 per breach or series of similar breaches discovered in a single investigation. *Private right of action?* —
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. 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.
Definition of Personal Information	Information containing an individual's first initial or first name and last name in combination with 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) *Exception:* 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 or is reasonably likely to occur and that creates a risk of harm to a person. *Exception:* 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 discovers or is notified of a security breach.

HAWAII

Notification of Data Subject	Yes, entity to which the statute applies shall provide notice to the affected individuals of a security breach.
Notification of Government	Yes, if 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	Yes, credit agency reporting is required if personal information for more than 1,000 people has been breached at a single time.
Notification by Third Parties	Yes, third parties must notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.
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 individuals • 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 notice must include a description of: • The incident in general terms; • The type of personal information that was subject to the unauthorized access and acquisition; • The general acts of the business or government agency to protect the personal information from further unauthorized access;

	• A telephone number that the person may call for further information and assistance, if one exists; and • Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. The covered entity may provide substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $100,000 • The number of affected individuals exceeds 200,000 • No sufficient contact information or consent for affected individuals • Affected individuals are unidentifiable *Alternate forms of notification:* • Email the affected individuals if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	There is a safe harbor for encrypted information, "the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key." *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 § 28-51-104 et seq.
Covered Entities	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 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 *Exception:* 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. *Exception:* 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.

IDAHO

Notification of Data Subject	Yes, covered entity shall give notice to the affected Idaho residents if there was a breach and misuse of information has occurred or is reasonably likely to occur. *Exception:* Notification is not required if after a good-faith, reasonable, and prompt investigation the covered entity determines that the misuse of information about an Idaho resident has not occurred or is not reasonably likely to occur.
Notification of Government	Yes, to the Idaho Attorney General's office within 24 hours of discovering a breach in addition to any responsibility to report to the chief information officer within the department of administration in accordance with Idaho authority policies.
Notification of Credit Reporting Agencies	No, notice to consumer reporting agencies is not required.
Notification by Third Parties	Yes, third parties must notify and cooperate with owner or licensee of information of any breach immediately following its discovery, if the personal information was misused or reasonably likely to be misused.
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 covered entity may provide substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $25,000 • The number of affected individuals exceeds 50,000 • Contact information for affected individuals is unavailable

	Substitute notice: • Email the affected individuals if their email address is available • Conspicuous disclosure of information on the covered entity's website, if available • Notify major statewide media
Exemptions or Safe Harbors	There is safe harbor for encrypted information. *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 or functional state or federal 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, there is no private right of action.
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	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 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. *Exception:* 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. *Exception:* If the personal information was retrieved in good faith.
Threshold for Notification	Upon the discovery or notification of a breach.
Notification of Data Subject	Yes, notice of breach must be given to Illinois residents affected by the breach.
Notification of Government	Yes, notice to the attorney general must be given for a breach to more than 500 Illinois residents in a single breach, including a description of the nature of the breach of security or unauthorized acquisition, number of Illinois residents affected by the incident at the time of notification, and any steps the Entity has taken or plans to take relating to the incident. *Exception*: Covered Entity subject to and in compliance with HIPAA.
Notification of Credit Reporting Agencies	Yes, but only with respect to state agencies. If a state agency must provide a notice of breach to more than 1,000 people at one time, they must also notify all consumer reporting agencies without unreasonable delay.
Notification by Third Parties	Yes, third parties must notify the owner or licensee of information of any breach immediately following discovery, if the personal information was or is reasonably believed to have been acquired by an unauthorized person.

ILLINOIS

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 provide a substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $250,000 • The number of affected individuals exceeds 500,000 • Contact information for affected individuals is unavailable *Substitute notice:* • Email the affected individuals if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media
Exemptions or Safe Harbors	There is safe harbor for encrypted information. *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? —
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 Practices Act if covered entities violate notification procedures. Remedies range from civil penalties of up to $50,000, to the cancellation of a covered entity's right to operate its business in Illinois. 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?* No, there is no express private right of action but private individuals may bring suit under the Illinois Consumer Fraud and Deceptive Businesses Practices Act.
Credit Monitoring Required	—

INDIANA

State and Statute	Indiana Code Ann. § 24-4.9-1-1 et seq.
Covered Entities	Database owners, including an individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity, that own or have the license to personal information in the form of computerized data.

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 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
	• Information collected by an adult-oriented website operator, or their designee
	Exception:
	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 of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an agency, individual, corporation, business trust, estate, trust, partnership, association, nonprofit or other legal or a commercial entity ("person"). The term includes the unauthorized acquisition of computerized data that has 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:*

INDIANA

	• 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	Upon discovery or notification of breach, where an Indiana resident's unencrypted personal information was or may have been acquired by an unauthorized person and the database 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	Yes, credit agency reporting required if information of more than 1,000 Indiana residents has been breached.
Notification by Third Parties	Yes, third parties must notify database owner if they discover that personal information was or may have been acquired by an unauthorized person.

INDIANA

Timing of Notification	Notifications must be sent without unreasonable delay, but not more than 45 days after the discovery of the breach. 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 The data collector may provide a substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $250,000 • The number of affected individuals exceeds 500,000 *Substitute notice:* • 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	There is a safe harbor for encrypted information, which is data that "have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key or are secured by another method that renders the data unreadable or unusable." *Following entity's own notification procedures?* Yes, as long as the privacy policy or security 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" any one or more of: • 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, there is no express private right of action.
Credit Monitoring Required	—

IOWA

State and Statute	Iowa Code § 715C.1-2 et seq.
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 a person's first name or first initial and last name in combination with 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 *Exception:* 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 acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. *Exception:*

	If the personal information was acquired in good faith by employees or agents for a legitimate purpose.
Threshold for Notification	Notice must be given upon discovery or receipt of notification of a breach. *Exception*: Notification is not required if, after conducting appropriate investigation or consulting with relevant federal, state, or local law enforcement agencies, determines "that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach."
Notification of Data Subject	Yes, person who owns or licenses computerized data that includes a consumer's personal information that was subject to a breach of security must give notice to any consumer whose personal information was included in the information that was breached.
Notification of Government	Yes, to the director of the Consumer Protection Division of the Office of the Attorney General within five (5) business days of breach if more than 500 Iowa residents are affected.
Notification of Credit Reporting Agencies	No, notice to credit reporting agencies is not required.
Notification by Third Parties	Yes, third parties must notify the owner or licensor of the information of any breach immediately following discovery.
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 provide a substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $250,000 • The number of affected individuals exceeds 350,000 • Contact information for affected individuals is unavailable *Alternate forms of notification:* • Email the affected individuals 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 statute 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 statute. • 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 civil penalties not exceeding $40,000, and seek additional damages on behalf of a person injured by a violation. *Private right of action?* No, there is no express private right of action, but the attorney general may seek damages on behalf of a private individual.
Credit Monitoring Required	—

KANSAS

State and Statute	Kansas Stat. Ann. § 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 consumer’s first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, 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 *Exception:* 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. *Exception:* 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.

KANSAS

Threshold for Notification	When the covered entity becomes aware of any breach of the security of the system and 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, notice is required to any Kansas resident where misuse of the resident's personal information has occurred or is reasonably likely to occur.
Notification of Government	No, notice to government agency is not required.
Notification of Credit Reporting Agencies	Yes, notice to credit agency reporting is required if notifications of a breach must be sent to more than 1,000 residents at once.
Notification by Third Parties	Yes, third parties must notify the owner or licensee of the information of breach following its discovery, provided that the personal information was or is reasonably believed to have been accessed and acquired 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 provide a substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $100,000 • The number of affected individuals exceeds 5,000 • Contact information for affected individuals is unavailable

KANSAS

	Alternate forms of notification: • Email the affected individuals 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 or functional state or 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, there is no private right of action.
Credit Monitoring Required	—

KENTUCKY

State and Statute	Kentucky Rev. Stat. § 365.732.
Covered Entities	Any person or business entity that conducts business in Kentucky.
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 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. *Exception:* 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	Upon discovery or notification of the breach in the security of the data.
Notification of Data Subject	Yes, any Kentucky resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person must be notified.
Notification of Government	No, notification to government agency is not required.

KENTUCKY

Notification of Credit Reporting Agencies	Yes, credit reporting agencies must be notified if notifications of a breach must be sent to more than 1,000 residents at once.
Notification by Third Parties	Yes, third parties must notify the owner or licensee of information "as soon as reasonably practicable following discovery" of any breach, if the personally identifiable information was, or is reasonably believed to have been, acquired 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 provide a substitute notice if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $250,000 • The number of affected individuals exceeds 500,000 • Contact information for affected individuals is unavailable *Substitute notice:* • Email the affected individuals 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?* No, there is no express government penalty for violations. However, a person may be able to recover under Ky. Rev. Stat. §446.070, which provides that "a person injured by violation of any statute may recover from the offender such damages as he sustained by reason of the violation." *Private right of action?* No, there is no express private right of action, but it may be available under Ky. Rev. Stat. §446.070, which provides that "a person injured by violation of any statute may recover from the offender such damages as he sustained by reason of the violation."
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 Louisiana 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 *Exception:* 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. *Exception:*

LOUISIANA

	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 (5) 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	—

LOUISIANA

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 affected individuals exceeds $100,000 • The number of affected individuals exceeds 100,000 • Contact information for affected individuals is unavailable *Alternate forms of notification:* • Email the affected individuals 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 Louisiana 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 Louisiana 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. *Exception:* 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 *Exception:* "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.

MAINE

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 an agency, individual, or a commercial entity. *Exception:* 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 Maine 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 Maine 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	Yes, third parties are 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 within 30 days after the breach and its scope is made aware.

	If law enforcement determines that the notification will not compromise a criminal investigation, the notification must be sent within seven (7) business days of that determination.
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 affected individuals exceeds $5,000 • The number of affected individuals exceeds 1,000 • Contact information for affected individuals is unavailable *Alternate forms of notification:* • Email the affected individuals 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.

MAINE

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 Maryland, 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

MARYLAND

	• A username or email address in combination with a password or security question and answer that permits access to an individual's email account • Genetic information *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 three (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 the Maryland Attorney General before providing consumer notice.

MARYLAND

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	Yes, third-party notification is required if covered entity maintains covered information on behalf of other entities 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 in 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 If there is a breach that allows access to an individual's email, electronic or other form of notice to individual to change account information is sufficient. 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 *Substitute notification:* The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $100,000 • The number of affected individuals exceeds 175,000 • Contact information for affected individuals is unavailable The substitute notice must: • Email the affected individuals if their email address is available • Conspicuous disclosure of information on the covered entity's website • Notify major statewide media

Exemptions or Safe Harbors	The Statute provides a safe harbor for encrypted information.
	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 its 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?* Yes, a violation of the data breach notification statute is an unfair or deceptive trade practice under Maryland's Consumer Protection Act, and any person injured as a result may bring action to recover damages and reasonable attorneys' fees.
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 *Exception:* "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 as long as the information is used for lawful purposes and not subject to further unauthorized disclosure.

MASSACHUSETTS

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 • 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 statute 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	Yes, 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, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (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, to the owner or licensor.
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 (3) business days. The covered entity may seek alternate forms of notification if one or more of the following situations occurs: • The cost of notifying affected individuals exceeds $250,000 • The number of affected individuals 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

MASSACHUSETTS

	Alternate forms of notification: • Email the affected individuals 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 the State of Michigan. 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's 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 *Exception:* "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.

MICHIGAN

	• 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	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. *Exception:* 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, notice must be given to any Michigan resident whose "unencrypted and unredacted personal information was accessed and acquired by an unauthorized person," or whose "personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key."
Notification of Government	—
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 must include the number of notices the person or agency provided to Michigan residents and the timing thereof.
Notification by Third Parties	Yes, 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.

MICHIGAN

Form of Notification	Covered entities must provide notification of a breach in one or more of the following ways: • Written notice • Electronic notice to the recipient if (1) the recipient has expressly consented to receive electronic notice, (2) 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, or (3) the person or agency conducts its business primarily through Internet account transactions or on the Internet. 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 individuals of the need to remain vigilant for fraud and identity theft Substitute notification is available if the cost of notifying entities exceeds $250,000, or the number of affected Michigan residents exceeds 500,000. Substitute notification must consistent of all of the following: • Email the affected residents 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 statute. 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
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 *Exception:* "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. *Exception:* 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.

MINNESOTA

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	Yes, 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	Yes, any person or business that maintains data that includes personal information that the person or business 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.
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.

MISSISSIPPI

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 or licenses personal information of Missouri residents, or any person that conducts business in Missouri that owns or licenses personal information of a Missouri resident. 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

MISSOURI

	• 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. The notice required by this statute 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
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.

MISSOURI

Notification of Credit Reporting Agencies	Yes, 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	Yes, a third party that maintains or possesses records or data containing personal information of Missouri residents that the person does not own or license, or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a Missouri resident that the person does not own or license, must notify the owner or licensee of the information of any breach of security immediately following its discovery, consistent with the legitimate needs of law enforcement.
Timing of Notification	Notice shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in this statute; 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. Statute provides a safe harbor for encrypted information.
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 statute for up to $150,000 per breach or series of similar breaches discovered at the same time.

	Private right of action? No, there is no private right of action.
Credit Monitoring Required	—

MONTANA

State and Statute	Montana Code Ann. § 30-14-1704
Covered Entities	Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information. "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 of the Montana Code Annotated.
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following when either the name or the data elements are not encrypted: • Social Security number • Driver's license number, state identification card number, or tribal identification card number • Account number, credit card, or debit card number, along with any required access code needed to access the financial account • Medical record information as defined in Montana Code Ann. § 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.

MONTANA

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 as long as that information is not used to further unauthorized disclosure.
Threshold for Notification	Disclosure of any breach of the security of the data system must be made 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 statute does not provide specific guidelines concerning the contents of the notification.
Notification of Government	Yes, any person or business that is required to issue a notification pursuant to this statute 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.
Notification of Credit Reporting Agencies	Yes, 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	Yes, third-party notice to owner or licensee of the information that was breached is required if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

MONTANA

Timing of Notification	The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity 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 $250,000, the number of affected individuals is greater than 500,000, or the business does not have sufficient contact information. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to local or statewide media
Exemptions or Safe Harbors	Following entity's own notification procedures, if they do not unreasonably delay notification. Statute provides a safe harbor for encrypted information.
Consequences of Non-Compliance	*Government enforcement?* Violation of the data breach notification statute is considered an unlawful practice as defined by the Montana Unfair Trade Practices and Consumer Protection Act of 1973. A willful violation may result in a civil fine of up to $10,000 per violation. Where there is a "fraudulent course of conduct," a fine may be imposed of up to $5,000 and imprisonment of up to one year, or both. *Private right of action?* No, there is no private right of action.
Credit Monitoring Required	—

NEBRASKA

State and Statute	Nebraska Rev. Stat. Ann. § 87-801
Covered Entities	An individual or commercial entity that conducts business in Nebraska, and that owns or licenses computerized data that includes personal information about a Nebraska resident.
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following when either the name or the data element are not encrypted, redacted, or otherwise altered by any method that renders the information unreadable: • Social Security number • Driver's license number or state identification card number • Account number, credit card, or debit card number, along with any required security code, access code, or password needed to access a resident's 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 government sources.
Definition of Breach	An unauthorized acquisition of unencrypted data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. *Exceptions:* • Good faith acquisition by an agent of a covered entity for the purposes of the covered entity if the personal information is not used 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 or order of a state agency

NEBRASKA

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.
Notification of Data Subject	Yes, a covered entity must give notice to any Nebraska resident if an investigation determines that the use of information about the resident for an unauthorized purpose has occurred or is reasonably likely to occur. The statute does not provide specific guidelines concerning the contents of the notification.
Notification of Government	Yes, to the attorney general not later than the time when it provides notice to the affected Nebraska resident.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Yes, an individual or commercial entity that maintains computerized data that includes personal information on behalf of the owner or licensee 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.
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 • Conspicuous posting on business's website • Notification to major statewide media Substitute notice is also permitted if the individual or commercial entity required to provide notice has ten

	employees or fewer and demonstrates that the cost of providing notice will exceed $10,000. The substitute notice may consist of: • Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents • Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the individual or commercial entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks • Conspicuous posting of the notice on the website of the individual or commercial entity if the individual or commercial entity maintains a website; and • Notification to major media outlets in the geographic area in which the individual or commercial entity is located.
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. The statute provides a safe harbor for encrypted information.
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 Nebraska resident injured by a statutory violation. *Private right of action?* No, there is no private right of action.
Credit Monitoring Required	—

NEVADA

State and Statute	Nevada Rev. Stat. Ann. § 603A.010 et seq.
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. *Exception:* A data collector that is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq.
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following when the name and data elements are not encrypted: • Social Security number • A driver's license number, driver authorization card number, or identification card number • Account number, credit card number, or debit card number, along with any required 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 by government records.
Definition of Breach	Any unauthorized acquisition of computerized data that materially 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 as long as the data is not used for purposes unrelated to the data collector or subject to further disclosure.

NEVADA

Threshold for Notification	Disclosure must be made following discovery or notification of the breach to any resident of Nevada whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Data Subject	Yes, any entity to which the statute applies shall disclose any breach in the security of the system data to any resident of Nevada whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Statute does not provide specific guidelines concerning the contents of the notification.
Notification of Government	—
Notification of Credit Reporting Agencies	Yes, credit agency reporting is required if more than 1,000 persons to be notified without unreasonable delay to any consumer reporting agency, as that term is defined in 15 U.S.C. § 1681a(p). The time and content of the notification must be provided.
Notification by Third Parties	Yes, 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.
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 does not have sufficient contact information. Substitute notice must consist of: • Email when possible • Conspicuous posting on business's website • Notification to major statewide media

Exemptions or Safe Harbors	Following entity's own notification procedures. Entities subject to the privacy provisions of the Gramm-Leach-Bliley Act. Statute provides a safe harbor for encrypted information.
Consequences of Non-Compliance	*Government enforcement?* The attorney general may bring an action for a temporary or permanent injunction if there is reason to believe that any person is violating, proposes to violate, or has violated the provisions of the notification statute. *Private right of action?* Yes, a data collector has a private right cause of action against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. Additionally, a person who is convicted of unlawfully obtaining or benefiting from personal information obtained as a result of a breach may be ordered to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the notification required by Nevada's data breach notification statute.
Credit Monitoring Required	—

NEW HAMPSHIRE

State and Statute	New Hampshire Rev. Stat. Ann. § 359-C:19 et seq.
Covered Entities	Any person doing business in New Hampshire who owns or licenses computerized data that includes personal information is subject to the statute's data breach notification requirements. Person is defined as an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state. Computerized data is defined as "personal information stored in an electronic format."
Definition of Personal Information	An individual's first name or first initial and last name, combined with one or more of the following when either the name or the data elements are not encrypted: • Social Security number • A driver's license number or other government identification number • Account, credit card, or debit card number, along with any required code needed to access an individual's financial account *Exception:* Information that is lawfully obtained from publicly available government records.
Definition of Breach	An unauthorized acquisition of data that compromises the security or confidentiality of personal information maintained by a person doing business in the state. This does not include the good-faith acquisition of personal information by an employee or agent of a person as long as the information is not used or subject to further unauthorized disclosure.
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.

NEW HAMPSHIRE

Notification of Data Subject	Yes, affected individuals must be notified when the covered entity becomes aware of a security breach and determines that misuse of the information has occurred or is reasonably likely to occur, or a determination cannot be made.
Notification of Government	Yes, a covered entity engaged in trade or commerce under N.H. Rev. Stat. Ann. § 358-A:3(I) must notify the regulator that has primary regulatory authority over such trade or commerce. All other persons must notify the New Hampshire's Attorney General's office. The notice must include the anticipated date of the notice to the individuals and the approximate number of individuals in New Hampshire who will be notified. The names of the individuals entitled to receive notice or any personal information relating to them is not required to be included in the notice.
Notification of Credit Reporting Agencies	Yes, credit agency reporting required if more than 1,000 persons to be notified. *Exception:* Covered entities that are subject to Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq.
Notification by Third Parties	Yes, any person or business that maintains computerized data that includes personal information that the person or business does not own must notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. *Exception:* If such cooperation shall be deemed to require the disclosure of confidential or business information or trade secrets.
Timing of Notification	Upon determining that misuse of the information has occurred or is reasonably likely to occur, or a determination cannot be made, the person shall notify affected individuals "as soon as possible," consistent with the legitimate needs of law enforcement.

NEW HAMPSHIRE

Form of Notification	Written, telephonic, or electronic (if the covered entity's primary means of communication with the affected individuals is by electronic means). Or substitute notice, if the cost of notification exceeds $5,000, the number of affected individuals is greater than 1,000, or the business does not have sufficient contact information or consent to provide the standard form of notice. 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 • The types of personal information that were or are reasonably believed to have been the subject of the breach 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. The statute provides a safe harbor for encrypted information. A covered entity that complies with the laws of state or federal regulators and acts according to the procedures for security breach notification is exempt.
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 to 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 and equitable relief and attorney's fees. If the violation was willful or knowing, the court shall award as much as three times, but not less than two times the amount of actual damages.

NEW HAMPSHIRE

Credit Monitoring Required	—

NEW JERSEY

State and Statute	New Jersey Stat. Ann. § 56:8-163
Covered Entities	Any business or public entity that compiles or maintains computerized records that include personal information. Business is defined as a sole proprietorship, partnership, corporation, association, or other entity, 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 New Jersey, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution. 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 • A driver's license number or state identification card number • Account, credit card, or debit card number, along with any required code needed to access the financial account • A user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account 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 government sources or widely distributed media.
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 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.

NEW JERSEY

	This does not include the good-faith acquisition of personal information by an employee or agent of a business that is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.
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. Disclosure is not required if the covered entity establishes that misuse of the information is not reasonably possible. The determination that misuse of the information is not reasonably possible must be documented in writing and retained for five (5) years.
Notification of Data Subject	Yes, covered entities shall disclose any breach of security to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.
Notification of Government	Yes, breaches must be notified to the Division of State Police in the Department of Law and Public Safety in advance of the disclosure to the affected individuals.
Notification of Credit Reporting Agencies	Yes, credit agency reporting is required if more than 1,000 persons are to be notified.
Notification by Third Parties	Yes, an entity that compiles or maintains computerized records that include personal information on behalf of another business or entity shall notify that entity of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.
Timing of Notification	In the most expeditious time possible, without unreasonable delay consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity 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 $250,000, the number of affected individuals is greater than 500,000, or the business does not have sufficient contact information.

	If the breach is for email login credentials, the notice must not be provided to that email address. If the breach only involves an individual's user name or password, in combination with any password or security question and answer that would permit access to an online account, and no other personal information, the business or public entity may provide the notification in electronic or other form that directs the breached customer to promptly change any password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the business or public entity and all other online accounts for which the customer uses the same user name or email address and password or security question or answer. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to major statewide media The statute does not specify the contents of a disclosure notice.
Exemptions or Safe Harbors	Following entity's own notification procedures. The statute provides a safe harbor for encrypted information.
Consequences of Non-Compliance	*Government enforcement?* A willful, knowing, or reckless violation of the notification statute constitutes an unlawful practice and a violation of Chapter 8 of New Jersey's' Trade Names, Trade Marks and Unfair Trade Practices statute (N.J. Stat. § 56:8-1 et seq.) and is subject to the remedies provided thereunder. Remedies the attorney general may seek under the statute include injunctive relief, civil penalties of not more than $10,000 for the first offense and not more than $20,000 for each later offense and costs incurred in connection with bringing the proceeding. A municipal or county office of consumer affairs also has enforcement authority. *Private right of action?* The statute does not expressly provide a private right of action.

Credit Monitoring Required	—

NEW MEXICO

State and Statute	New Mexico 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 code or password that would permit access to a person's financial account • Biometric data *Exception:* 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. *Exception:* The good-faith acquisition of personal information by an employee or agent of a business as long as the information is not subject to further unauthorized disclosure.
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.

	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 each New Mexico resident whose personal identifying information is reasonably believed to have been subject to the breach and that breach gives rise to a significant risk of identity theft or fraud. The notice must contain: • 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 Notice is not required if, after an appropriate investigation, it is determined that the security breach does not give rise to a significant risk of identity theft.
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, the covered entity shall notify the Office of the Attorney General in the most expeditious time possible, and no later than 45 calendar days. The attorney general must be notified of the number of New Mexico residents that received notice and provide a copy of the notice that was sent to affected residents.
Notification of Credit Reporting Agencies	Yes, credit agency reporting is 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.

NEW MEXICO

Notification by Third Parties	Yes, 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 is not required if, after an appropriate investigation, the third-party agent determines that the security breach does not give rise to a significant risk of identity theft or fraud.
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 (electronic notices must be consistent with 15 U.S.C. § 7001 or it must be that the covered entity primarily communicates with the New Mexico resident by electronic means). Or substitute notice, if the cost of notification exceeds $100,000, the number of affected individuals is greater than 50,000, or the covered entity does not have a physical address record or sufficient contact information for the residents that must be notified. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to major media outlets in New Mexico and the attorney general
Exemptions or Safe Harbors	Following entity's own notification procedures consistent with the timing requirements of the statute. The statute provides a safe harbor for encrypted information. *Exemptions:* A person subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996.

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 of: • $25,000 or • $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 § 208 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 or nondriver identification card number • Account, credit card, or debit card number, along with any required 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 email address in combination with a password or security question and answer that would permit access to an online account

NEW YORK

	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 as long as the information is not used or subject to unauthorized disclosure.
Threshold for Notification	Disclosure is necessary following the discovery or notification of the breach where a covered entity believes that private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. *Exception:* Notice is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected individuals or emotional harm in the case of unknown disclosure of online credentials. Such a determination must be documented in writing and maintained for at least five (5) years. If the incident affects over 500 residents of New York, the person or business shall provide the written determination to the state attorney general within 10 days after the determination.
Notification of Data Subject	Yes, a covered entity must give notice of a breach 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.
Notification of Government	Yes, if any New York residents are notified, the state attorney general must be notified and provided with a copy of the template notice to be provided to residents and the approximate number of affected individuals.
Notification of Credit Reporting Agencies	Yes, credit agency reporting is required if more than 5,000 New York residents are notified.

NEW YORK

Notification by Third Parties	Yes, 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.
Timing of Notification	The most expeditious time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach.
Form of Notification	Written, telephonic (and a log of each notification), or electronic (if electronic, there must be express consent for electronic notice and a log of each notification). Or substitute notice, if the cost of notification exceeds $250,000, the number of affected individuals is greater than 500,000, or the business does not have sufficient contact information for affected individuals. 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; and • Notification to major statewide media. The notice should include: • Contact information for the person or business making the notification; • The telephone numbers and websites of relevant state and federal agencies that provide information regarding security breach response, identity theft prevention, and protection information; and • A description of the types of information that were, or are reasonably believed to have been, accessed or acquired, including the specification of which of the elements of personal and private information were, or are reasonably believed to have been, so accessed or acquired.
Exemptions or Safe Harbors	Additional notice not required if notice is given under Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809) or regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164). The statute provides a safe harbor for encrypted information.

Consequences of Non-Compliance	*Government enforcement?* The attorney general may bring an action seeking injunctive relief and, in connection with such action, a court may award damages incurred by a person who was not given notice of a security breach. In cases of knowing or reckless violation of the statute, the court may impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, provided that the latter amount does not exceed $250,000. *Private right of action?* No.
Credit Monitoring Required	—

NORTH CAROLINA

State and Statute	NC. Gen. Stat. § 75-60 et seq.
Covered Entities	Any sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise). 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 any of the following: • 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 • Digital signatures • Any other numbers or information that can be used to access a person's financial resources • Biometric data • Fingerprints • Password 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 government sources or information that an individual has voluntarily consented to have publicly disseminated or listed on publicly available directories.
Definition of Breach	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. Or, unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. This does not include the good-faith acquisition of personal information by an employee or agent of a business as long as the information is used for a lawful purpose of the business and not subject to further unauthorized disclosure.
Threshold for Notification	Discovery or notification of the breach.
Notification of Data Subject	Yes, clear and conspicuous notice must be given to affected individuals any time a business discovers or is given notice of a security breach. It must 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 individuals can call for further information and assistance • Advice directing affected individuals 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 individuals can obtain information about preventing identity theft from and the toll-free telephone numbers, addresses, and website

	addresses of the Federal Trade Commission and the North Carolina Attorney General's Office Any business that possesses records containing PI of residents of North Carolina that the business does not own or license or conducts business in North Carolina 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, when a covered entity notifies affected individuals, it must also notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office. The notice must include the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.
Notification of Credit Reporting Agencies	Yes, credit agency reporting is required to the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notices if more than 1,000 persons are notified under this statute.
Notification by Third Parties	Yes, any business that maintains or possesses records or data containing personal information of North Carolina residents that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license, must notify the owner or licensee of the information of any security breach immediately following discovery of the breach.
Timing of Notification	Without unreasonable delay, consistent with the legitimate needs of law enforcement or as necessary to determine sufficient contact information or to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.
Form of Notification	Written, telephonic (if contact is made directly with the affected individuals), or electronic (if electronic, consistent with 15 U.S.C. § 7001 and the recipient must have agreed to receive communications electronically). Or substitute notice, if the cost of notification exceeds $250,000, the number of affected individuals is greater than

	500,000, or if there is insufficient contact information or consent. Substitute notice must consist of: • Email • Conspicuous posting on business's website • Notification to major statewide media
Exemptions or Safe Harbors	Financial institutions are considered to be in compliance with this statute if they are in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. A credit union is deemed to be in compliance with the statute if it "is subject to and in compliance with the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration." The statute provides a safe harbor for encrypted information.
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 or violations of court orders. 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	N.D. Cent. Code § 51-30-01 et seq.
Covered Entities	Any person that owns or licenses computerized data that includes personal information.
Definition of Personal Information	An individual's first name or initial and last name, in conjunction with any of the following when the name and data elements are not encrypted: • Social Security number • Operator's license number assigned to an individual by the department of transportation under N.D. Cent. Code § 39-06-14 • Nondriver color photo identification card number assigned to the individual by the department of transportation under N.D. Cent. Code § 39-06-03.1 • Financial institution, credit, and debit card account numbers in combination with a code that would permit access to an individual's financial accounts • Date of birth • The maiden name of the individual's mother • Health insurance or medical information • Employer ID in combination with any required security code, access code, or password • Digitized or electronic signature *Exception:* "Personal information" does not include publicly available information lawfully obtained from 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. *Exception*: Good-faith acquisition of an individual's personal information by an employee or agent of the individual provided the data is not used or subject to further unauthorized disclosure.

NORTH DAKOTA

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 following discovery or notification of the breach. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the integrity of the data system. 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 the discovery or notification of a breach of the security system.
Notification of Government	Yes, if more than 250 individuals are notified.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Yes, any persons maintaining computerized personal data on behalf of another must notify the owner or licensee of any breach immediately, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person.
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, or in accordance with any measures necessary to determine the scope of the breach and to restore the integrity of the data system.
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 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 covered entity does not have sufficient contact information. 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 The statute does not provide specific guidelines for the contents of the notification.
Exemptions or Safe Harbors	A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is deemed to be in compliance with the statute. N.D. Cent. Code § 51-30-06. 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. The statute provides a safe harbor for encrypted information.
Consequences of Non-Compliance	*Government enforcement?* The attorney general may seek injunctive relief, appointment of a receiver, civil penalties of not more than $5,000 for each violation, and reasonable attorney's' fees, investigation fees, costs, and expenses of the investigation and the action. The attorney general may also issue a cease and desist order where necessary or appropriate in the public interest, and may impose a civil penalty of up to $1,000, for each violation against a person found to have violated a cease and desist order. Any other remedies under the state's consumer protection law is also available. *Private right of action?* A private right of action may be available under the state's consumer protection statute.
Credit Monitoring Required	—

OHIO

State and Statute	OH. REV. CODE ANN. § 1349.19 et seq.
Covered Entities	Any "person that owns or licenses computerized data that includes personal information." The definition of "person" explicitly includes business entities that conduct business in Ohio (but those who do not are excluded from the definition).
Definition of Personal Information	An individual's name (or first initial and last name) combined with any one or more of the following 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 identification card number • Account number on a credit or debit card, in combination with any security code or password that would permit access to an individual's financial account *Exception:* "Personal information" explicitly does not include: • Any information gathered from a news source • Any information shared amongst a bona fide association or charitable/fraternal nonprofit organization • Any media similar to those listed above • Any publicly available information that is lawfully made available to the general public by federal, state, or local government records.
Definition of Breach	Any unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information that is reasonably believed to have caused or reasonably believed that it will cause, material risk of identity theft or other fraud for a resident of Ohio. This definition explicitly excludes good faith acquisitions of personal information by an employer or agent provided that the information is not used for an unlawful purpose or subject to a further disclosure. It also excludes searches predicated on warrants, subpoenas, court orders, and regulatory oversight.
Threshold for Notification	Must disclose the breach following its discovery or notification of the 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 it is reasonably believed to cause a material risk of identity theft or other fraud.
Notification of Data Subject	Yes, must disclose the breach to any resident of Ohio whose data is breached "in the most expedient time possible," but within 45 days of the breach.
Notification of Government	Only if the covered entity was acting on behalf of, or at the direction of, the government when the breach occurred.
Notification of Credit Reporting Agencies	Yes, if more than 1,000 residents of Ohio are affected by a security breach, all consumer reporting agencies must be notified "without unreasonable delay." The disclosures to data subjects explicitly cannot be delayed in order to make the required notifications to consumer reporting agencies.
Notification by Third Parties	—
Timing of Notification	**For data subject:** "In the most expedient time possible," but within 45 days of the breach. **For consumer reporting agencies:** "without unreasonable delay." Either of these notification timeframes can be delayed if a law enforcement agency determines that the disclosure would impede criminal investigations or jeopardize homeland or national security. In such a case, law enforcement is entitled to set a timeline.
Form of Notification	Notice may be provided (1) in writing, (2) electronically, or (3) via telephone. 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 covered entity has insufficient contact information for the affected class. Substitute notice may be: • Email if the subject has an email address • Conspicuous posting on the entity's website • Notification of major media outlets to the extent the total readership/viewing audience is greater than or equal to 75% of the state.

	If the company has less than 10 employees, and the costs of notice will exceed $10,000, it may provide substitute notice in the following ways: • Include a paid advertisement in the local newspaper, covering at least one quarter of the page, at least once a week for three (3) consecutive weeks • Include a conspicuous posting on the company's website • Notification of the major media outlets where the entity is located The notification can also be done pursuant to existing contract so long as it does not conflict with the provisions of the statute.
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 statute. Any covered entity subject to HIPAA is exempt from this statute. 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	*Government enforcement?* The attorney general has the exclusive authority to bring a civil action for violation of the statute, which can include a temporary restraining order, preliminary or permanent injunction, and civil penalties. Any covered entity who violates the statute is subject to a penalty of up to $1,000 per day for each day the covered entity fails to comply with the statute. If the covered entity has

	intentionally or recklessly failed to comply for more than 60 days, the civil penalty can be up to $1,000 per day for the first 60 days and $5,000 for every day thereafter. An additional penalty of $10,000 per day may be charged after non-compliance for 90 days. *Private right of action?* No, there is no private right of action.
Credit Monitoring Required	—

OKLAHOMA

State and Statute	OK STAT. tit. 24 § 161 et seq.
Covered Entities	Any individual or entity that owns or licenses computerized data that includes personal information. "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit.
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 that relate to a resident of Oklahoma, when the data elements are neither encrypted nor redacted: • Social Security number • Driver's license number or state identification card number • Any financial, credit, or debit account number in combination with any required security code or password that would permit access to the accounts of an Oklahoma resident The definition explicitly excludes information 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 access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of any personal information maintained by an individual or an entity as part of a database of personal information regarding multiple individuals and that causes, or is reasonably believed will cause identity theft or other fraud to any resident of Oklahoma. This definition explicitly excludes good faith acquisitions of personal information by an employee or agent, so long as it is not used for a purpose that is unlawful or subject to further disclosure.
Threshold for Notification	Must disclose if there is a breach of a security system holding personal information if that breach includes unredacted or unencrypted personal information, or is reasonably believed to have included such, that one

	reasonably believes will cause or has caused identity theft or other fraud for a resident of Oklahoma. If the material is encrypted, but the breach also includes the key to unencrypt, notification is required.
Notification of Data Subject	Yes, the data subject must be notified of a breach "without unreasonable delay."
Notification of Government	No, unless business is subject to oversight of state Real Estate Commission.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Yes, if an entity maintains data on behalf of another owner or licensee, any breach must be disclosed to the owner or licenser of the data "as soon as practicable."
Timing of Notification	**For data subjects:** notification must be made "without unreasonable delay." Notification required under this statute may be delayed if a law enforcement agency determines that giving the subject notice would impede a criminal or civil investigation or national security. After law enforcement has decided to permit notification, it must be done "without unreasonable delay."
Form of Notification	Notice can be written and mailed, given by telephone, given electronically, or, if the notification would cost over $50,000 or the affected class exceeds 100,000 people, the entity can give substitute notice instead. Substitute notice consists of any two of the following: • Emailing notice • Conspicuous posting of notice on the website of the company • Notifying major statewide media
Exemptions or Safe Harbors	If an entity has its own notification procedure pursuant to a privacy or security policy, that notification method may be used so long as it is consistent with the timing requirements of the statute.

	Financial institutions that comply with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Consumer Notice is deemed to be in compliance with the provisions of the statute. Any entity that complies with the notification requirements of their federal regulator is deemed compliant.
Consequences of Non-Compliance	*Government enforcement?* A violation of the statute that results in injury or loss to the residents of the state may be enforced by the attorney general or district attorney as an unlawful practice under the Oklahoma Consumer Protection Act. The penalties may be actual damages or civil penalties. If the latter, maximum penalty per breach event (or series of breaches under one investigation) is $150,000. *Private right of action?* No, there is no private right of action.
Credit Monitoring Required	—

OREGON

State and Statute	OR. REV. STAT. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626
Covered Entities	Any person (i.e., 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) that owns, licenses, maintains, stores, manages, collects, processes, acquires, or otherwise possesses personal information in the course of business, vocation, occupation, or volunteer activities. This does not include someone who acts solely as a vendor. "Vendor" means a person with which a covered entity contracts to maintain, store, manage, process or otherwise access personal information for the purpose of, or in connection with, providing services to or on behalf of the covered entity.
Definition of Personal Information	A consumer's first name or first initial and last name in combination with any of the following, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired: • Social Security number • Driver's license number or other state identification number issued by the Department of Transportation • Passport number or other identification issue by the United States • Any credit or debit card number or account number in conjunction with the required security code or password that would permit access to a financial account, or any other information that a person reasonably knows or should know will permit access to a consumer's financial accounts • 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 • Any health insurance identification or policy number in combination with any unique identifier that is used to identify the customer

OREGON

	• 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 A user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification. Additionally, any of the aforementioned data elements without the combination with a name or user name if encryption or redaction techniques have not been used and the information obtained would enable a person to commit identify theft against the state resident whose information was compromised. *Exception*: This definition does not include any data in government records lawfully made available to the public (except SSN).
Definition of Breach	An unauthorized acquisition of computerized data that materially compromises security, confidentiality, or integrity of personal information that a person maintains or possesses. *Exception*: This does not include inadvertent acquisitions by a person or a person's employee or agent so long as that employee or agent does not use the information in violation of the law or in a manner that poses a threat to or harms the security, confidentiality, or integrity of the personal information.
Threshold for Notification	If a covered person is subject to a breach, or a vendor gives them notice of a breach, there must be notification to the subject of the breach. *Exception*: A covered person does not need to notify consumers of a breach of security if, after an appropriate investigation or after consultation with relevant federal, state or local law enforcement agencies, the covered entity reasonably determines that the consumers whose personal information was subject to the breach of security are unlikely to suffer harm. The covered person must document the determination in writing and maintain the documentation for at least five (5) years.

OREGON

Notification of Data Subject	Yes, if there is a breach, or a vendor gives notice to a covered entity that there has been a breach, any individual whose information was included in the breach must be notified, "without unreasonable delay," but not longer than 45 days after the breach. If a vendor (not a covered entity) has a breach, or reasonably believes that they have had a breach, related to a covered entity's data, they must notify the covered entity as soon as practicable but not later than 10 days.
Notification of Government	Yes, if a breach affects more than 250 individuals, the attorney general must be given a copy of each notice given to a consumer. This specific requirement is not subject to the exemptions set forth in the "Safe Harbor/Exemptions" column.
Notification of Credit Reporting Agencies	Yes, if a security breach affects more than 1,000 consumers, the covered entity must alert, "without unreasonable delay," all consumer reporting agencies of the timing, distribution, and content of the notices distributed.
Notification by Third Parties	Yes, a vendor that discovers a breach of security or has reason to believe that a breach of security has occurred shall notify a covered entity with which the vendor has a contract as soon as is practicable but not later than 10 days after discovering the breach of security or having a reason to believe that the breach of security occurred. A vendor shall notify the attorney general in writing or electronically if the vendor was subject to a breach of security that involved the personal information of more than 250 consumers or a number of consumers that the vendor could not determine, unless the relevant covered entity has already notified the attorney general. If a vendor, who has a contract with another vendor, who has a contract with the covered entity, the intermediary vendor must be notified.
Timing of Notification	**For data subject:** "in the most expeditious manner, without unreasonable delay" and not more than 45 days after the breach. **For government:** "without unreasonable delay." **For consumer reporting agencies:** "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 may be in writing, electronic (if that is how the entity customarily communicates with the consumer), or by telephone. Notification must include: • A description of the breach • The approximate date of the breach • The type of personal information subject to the breach • The contact information of the covered entity • The contact information for national consumer reporting agencies • Advice to the consumer to report suspected identity theft to law enforcement, the attorney general, and FTC Substitute notice may be provided in the event that the breach affects 350,000 consumers or notification would cost over $250,000. Substitute notice may consist of: • Posting a notice or link to a notice on the covered person's website • Notifying major statewide television and newspaper media.
Exemptions or Safe Harbors	The statute does not apply to: • Personal information that is subject to, and a person that complies with, notification requirements or procedures for a breach of security that the person's primary or functional federal regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance. • Personal information that is subject to, and a person that complies with, a state or federal law that provides greater protection to personal information and disclosure requirements at least as thorough as the protections and disclosure requirements provided under this statute. • A covered entity or vendor that complies with regulations promulgated under Title V of the Gramm-Leach-Bliley Act of 1999. • A covered entity or vendor that complies with regulations promulgated under HIPAA.

Consequences of Non-Compliance	*Government enforcement?* The director of the Department of Consumer and Business Services may engage in investigations, issue subpoenas, or compel production of materials. Additionally, if the Director believes that noncompliance is occurring or has occurred, the Director may issue a cease and desist order or require the violating party to pay compensation to the victims (to do this there must be a finding that enforcement of the rights by private civil action would be too burdensome to be practical). Any person who violates or procures, aids or abets in a violation of the statute is subject to a penalty of not more than $1,000 for every violation. Under this rule, each violation is a separate offense, and each day's continued noncompliance is a separate violation, but the maximum penalty is $500,000. *Private right of action?* No, there is no express private right of action.
Credit Monitoring Required	If there is a fee affiliated with credit monitoring offered by the entity, it must be disclosed.

PENNSYLVANIA

State and Statute	73 PA. STAT. § 2301 et seq. (as amended by S.B. 696)
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 in combination with any of the following in an unencrypted or unredacted form: • Social Security number • Driver's license number or a state identification card number issued in lieu of a driver's license • Financial account number, credit or debit card number, in combination with any password, access code or security code, which would permit access to an individual's financial account • Medical information • Health insurance information • A user name or email address, in combination with a password or security question and answer that would permit access to an online account This explicitly does not include publicly available information that is lawfully made available to the general public from government records or widely distributed media.
Definition of Breach	Unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as a part of a database of personal information regarding multiple individuals and that causes, or the entity reasonably believes has or will cause loss or injury to any Pennsylvania resident.
Threshold for Notification	An entity shall provide notice of any breach of the security of the system following determination of a breach of the security system, when unredacted, unencrypted personal information was, or is reasonably believed to have been accessed and acquired by an unauthorized person. Encrypted information is treated as unencrypted when an encryption key was also subject to the breach.

PENNSYLVANIA

	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.
Notification of Data Subject	Yes, upon a breach of security, an entity must notify data subjects "without unreasonable delay" if their personal information was accessed by an unauthorized party. However, delay is permissible at the advice of law enforcement or to determine the scope of a breach and maintain the system's integrity.
Notification of Government	Yes, if 500 Pennsylvania residents must be notified, the entity must give notice concurrently to the attorney general that includes the following: • The organization name and location • The date of the breach of the security system • A summary of the breach incident • An estimated total number of affected individuals • An estimated total number of individuals in Pennsylvania affected by the breach
Notification of Credit Reporting Agencies	Yes, if more than 500 individuals must be notified, the entity must also notify all consumer reporting agencies "without unreasonable delay."
Notification by Third Parties	Yes, a vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security of the system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data.
Timing of Notification	**For data subjects:** "without unreasonable delay," though delay is permitted in order to determine the scope of the breach and maintain the integrity of the system. **For the government:** Notification must be given "concurrently" with notification to residents. **For consumer reporting agencies:** "without unreasonable delay." All of the notification requirements under this act may be delayed if a law enforcement agency determines and advises the entity in writing, referencing this statute, that the notification will impede an investigation or national or homeland security. After law enforcement determines that the notification will no

	longer impede the investigation or security, notification shall be made by the entity.
Form of Notification	Notification may be made in written, telephonic, email, or electronic form. In order to make notification through email, there must be a prior business relationship and a valid email address. In order to make notification electronically, the notice must direct the person to promptly change their password and security question or answer, as applicable, or take other steps appropriate to protect the person's online account. The entity may provide substitute notice instead of the above methods if it demonstrates that the costs of providing notice would exceed $100,000, the affected individuals exceeds 175,000, or the entity does not have sufficient contact information. Substitute notice may consist of: • Email notice when the entity has an email address • Conspicuous posting on the entity's internet website if the entity maintains one • Notification of major statewide media
Exemptions or Safe Harbors	An entity subject to and in compliance with HIPAA shall be deemed in compliance with this chapter. If an entity maintains its own notification procedures as a part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of the statute, the entity is deemed to be in compliance with the statute, if it notifies its customers in compliance with this policy. 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 compliant. A state agency, or a state agency's contractor, that complies with the notification requirements of its primary state or functional federal regulator is deemed in compliance with this chapter.
Consequences of Non-Compliance	*Government enforcement?* The attorney general has the exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law. *Private right of action?*

	No, there is no private right of action.
Credit Monitoring Required	The entity must provide access to one independent credit report from a consumer reporting agency if the individual is not eligible to obtain an independent credit report for free under 15 U.S.C. 1681. Additionally, the entity must provide access to free credit monitoring for the 12-month period following the notification. This is satisfied by informing the individual of the availability of this free credit monitoring. This provision applies only if the entity believes that the first name or initial and last name of an individual has been accessed by an unauthorized party along with a Social Security number, bank account number, or driver's license or state ID number.

PUERTO RICO

State and Statute	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 organizations of the three branches of government, corporations, partnerships, associations, private companies, or organizations authorized to do business in Puerto Rico.
Definition of Personal Information	The first name or initial and last name of an individual combined with any of the following information so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code: • Social Security number • Driver's license number, voter identification, or other official identification • Bank or financial account numbers with or without passwords or access codes needed to access them • User names and passwords or access codes to public or private information systems • Medical information protected by HIPAA • Tax information • Work-related evaluations Any residential address or information in public documents and available to citizens in general is explicitly excluded from this definition.
Definition of Breach	Any situation where access has been permitted to unauthorized persons or entities to data files so that the security, confidentiality or integrity of the information (or that this is reasonably believed to have occurred). Additionally, if an authorized person or entity is known or reasonably suspected to have violated professional

	confidentiality or obtained authorization under false pretenses with the intention of making illegal use of the information. This can be both system access or physical access to the recording media coupled with undue removal or retrieval of those recordings.
Threshold for Notification	A notification must be made to data subjects and the Department of Consumer Affairs when a breach includes personal information if it is unencrypted (though password protected files being breached still requires notification).
Notification of Data Subject	Yes, the entity must notify the data subjects "as expeditiously as possible," taking into account the needs of law enforcement to secure evidence and crime scenes as well as needing to restore the system's security.
Notification of Government	Yes, the entity must notify the Department of Consumer Affairs within a non-extendable period of 10 days, who, in turn, must make a public announcement within 24 hours.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	—
Timing of Notification	**For data subjects:** Must be notified "as expeditiously as possible" while taking into account the needs of law enforcement and the application of measures needed to restore the system's security. **For Department of Consumer Affairs:** Not later than 10 days after the breach has been detected.
Form of Notification	Must be provided in a clear and conspicuous manner and describe the breach and the information compromised. The notification also must include a toll free number and website for affected individuals to use to obtain information or assistance. Notice can be given: • In written form • Authenticated electronic means (according to the Digital Signatures Act)

	If the cost of giving notice or identifying individuals to whom notice should be given would be "excessively onerous," exceeds $100,000, or the number of people who must be notified exceeds 100,000, the entity may give notice by doing both of the following: • Prominent display of an announcement to that respect at the entity's premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic; and • A communication to the media informing them of the breach and providing information on how to contact the entity. If the breach is specific to a sector, publications circulated in that sector may be used.
Exemptions or Safe Harbors	No provision of the statute shall be interpreted as being prejudicial to those institutional information and security policies that an enterprise or entity may have in force prior to the date of the statute and whose purpose is to provide protection equal or better to the information on security established by the statute.
Consequences of Non-Compliance	*Government enforcement?* The Secretary may impose fines of $500, up to a maximum of $5,000 for each violation. *Private right of action?* Yes, any government-imposed fines do not affect the rights of the consumers to initiate actions or claims for damages.
Credit Monitoring Required	—

RHODE ISLAND

State and Statute	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	An individual's first name or initial and last name in combination with any one or more of the following data elements in their unencrypted form: • Social Security number • Driver's license number, state-issued identification number, or tribal identification number • Account number, credit or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account • Medical or health insurance information • Email address with any required password or access code that would provide access to an individual's personal, medical, insurance, or financial account *Exception:* 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	Unauthorized access or acquisition of unencrypted computerized information that compromises the security, confidentiality, or integrity of personal information maintained by the covered entity. Good faith acquisition of personal information by an employee or agent of a state agency is not a breach of security provided that the information is not used or subject to further unauthorized disclosure.
Threshold for Notification	An entity must provide notification in accordance with this chapter any time there is a disclosure of personal information, or a breach of the security system, that poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity.

RHODE ISLAND

Notification of Data Subject	Yes, notification shall be given to data subjects "in the most expedient time possible," but not longer than 45 days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements.
Notification of Government	Yes, in the event that more than 500 Rhode Island residents are to be notified, the person shall notify the attorney general as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general shall be made without delaying notice to affected Rhode Island residents.
Notification of Credit Reporting Agencies	Yes, in the event that more than 500 Rhode Island residents must be notified. The person shall notify the credit reporting agency as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general shall be made without delaying notice to affected Rhode Island residents.
Notification by Third Parties	Yes, the breach notification requirements apply to any person that "acquires, uses, or licenses data that includes personal information."
Timing of Notification	**For data subjects:** "in the most expedient time possible," but not longer than 45 days. **For the government:** "without unreasonable delay" **For consumer reporting agencies:** "without unreasonable delay" *Exception*: The notification may be delayed if a federal, state, or local law enforcement agency determines that the notification will impede a criminal investigation.
Form of Notification	Notice may be provided by: • Written notice • Electronic notice (if compliant with 15 U.S.C. § 7001) If providing the notification would cost more than $25,000 or more than 50,000 Rhode Island residents were affected, the entity may notify by doing all of the following: • Email notice, if the entity has email addresses for the subjects; • Conspicuous posting of notice on the entity's website; and • Notification of major statewide media.

	The notification must include: • A general and brief description of the breach, including how it occurred and the number of affected individuals • The type of information that was subject to the breach • The date of the breach • The date that the breach was discovered • A description of the remediation services offered, if any, including toll free numbers and websites to contact credit reporting agencies, remediation service providers, and the attorney general • A description of the consumer's ability to file or obtain a police report, how a consumer requests a security freeze, and the fees that may need to be paid to consumer reporting agencies
Exemptions or Safe Harbors	An entity is deemed to be in compliance with the statute if it: • Maintains its own security breach procedures as a part of an information security policy that complies with the timing requirements of the chapter and notifies the subjects in accordance with such policies • Is a financial institution, trust company, credit union, or affiliate thereof in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Consumer Notice • Maintains a security breach procedure that is pursuant to the rules established by their primary or functional regulator and notifies all subject persons as required by that regulator • Is a covered entity under HIPAA that is subject to the rules established by the Department of Health and Human Services regarding medical privacy and security rules
Consequences of Non-Compliance	*Government enforcement?* Each **reckless** violation may be punished by a civil penalty of no more than $100 per record. Each **knowing and willful** violation may be punished by a civil penalty no more than $200 per record. If the attorney general believes that a violation of the statute has occurred and that bringing suit would be in the public

	interest, it may bring an action in the name of the state against the entity. *Private right of action?* No, there is no private right of action for the individual.
Credit Monitoring Required	—

SOUTH CAROLINA

State and Statute	SC 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 initial and last name of an individual combined with any of the following information: • Social Security number • Driver's license number or state identification number issued instead of a driver's license • Credit card, debit card, or financial account numbers in combination with any required security code, access code, or password that would permit access to a resident's financial account • Numbers or information that may grant access to a person's financial accounts • Numbers or information issued by a government or regulatory entity that uniquely identifies an individual The definition explicitly excludes information that is lawfully obtained from publicly available information, or from federal, state, or local governmental records lawfully made available to the general public.
Definition of Breach	Unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident. *Exception*: Good faith acquisition of personal identifying information by an employee or agent of the person for the purposes of its business is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.

SOUTH CAROLINA

Threshold for Notification	Upon the breach of a security system that includes the personal identifying information of a resident that was not made unusable by encryption, redaction or other methods, if acquired by an unauthorized individual that has or is reasonably likely to result in illegal use of the information or use that would create a material risk of harm to the resident.
Notification of Data Subject	Yes, notification must be made upon breach "in the most expedient time possible and without unreasonable delay."
Notification of Government	Yes, if 1,000 residents or more must be notified, the Consumer Protection Division of the Department of Consumer Affairs must be notified of the timing, distribution, and content of the consumer notices "without unreasonable delay."
Notification of Credit Reporting Agencies	Yes, if 1,000 people or more must be notified, all consumer reporting agencies must be notified of the timing, distribution, and content of the consumer notices "without unreasonable delay."
Notification by Third Parties	—
Timing of Notification	**For data subjects:** The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. **For the government:** "without unreasonably delay" **For consumer reporting agencies:** "without unreasonable delay" *Exception:* Notification may be delayed if a law enforcement agency determines that notification would impede a criminal investigation. Notification must then be made after it no longer compromises the investigation.
Form of Notification	Notice may be given in writing; electronically, if the person's primary method of communication with the individual is by electronic means; or telephonically. However, if the person demonstrates that providing notice would exceed $250,000, that the affected class exceeds 500,000 individuals, or that the person has insufficient contact information, they may provide substitute notice.

	Substitute notice requires: • Providing email notice • Posting a conspicuous notice on the website, or • Notification to major statewide media
Exemptions or Safe Harbors	If a person or organization maintains its own notification procedures pursuant to a security policy that are consistent with the timing requirements of the statute and the subjects are notified in compliance with that policy, they are deemed to be compliant with the statute. The statute does not apply to any financial institution that is subject to and in compliance with the privacy and security provisions of the Gramm-Leach-Bliley Act or the federal Interagency Response Programs for unauthorized Access to Consumer Information and Customer Notice issued March 7, 2005.
Consequences of Non-Compliance	*Government enforcement?* The knowing and willful violation of the statute can result in a fine of $1,000 for each resident whose information was accessible by reason of the breach. *Private right of action?* Yes, a resident who is injured by a violation of the statute may institute a civil action to recover damages in the case of a willful and knowing violation, recover actual damages in the case of a negligent violation, seek an injunction, and recover attorneys' fees or costs if successful.
Credit Monitoring Required	—

SOUTH DAKOTA

State and Statute	S.D. CODE ANN. (§§ 22-40-19 et seq.)
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.
Definition of Personal Information	**Personal information** is an individual's first name or initial and last name, combined with any of the following: • Social Security number • Driver's license number or other unique identification number created or collected by a government body • Account, credit card, or debit card number in combination with any required access code, password, PIN, routing number, or any other information required to access a person's account • Health information as defined by HIPAA • An identification number given by an employer in combination with any security/access code, password, or biometric data generated from measurements or analysis of human body characteristics used for authentication purposes The term does not include information made lawfully available through government records, or information redacted or made otherwise 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, debit card, or credit card number in combination with any required security/access code, password, PIN or any other information required to access a person's account
Definition of Breach	Unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the covered entity. This does not include good faith acquisition by an employee or agent so long as it is not used or subject to further unauthorized disclosure.

SOUTH DAKOTA

Threshold for Notification	If the information of the resident of the state is or is reasonably believed to have been acquired by an unauthorized individual, they must be given notice. However, notification does not have to be given if, after an investigation and notice to the attorney general, the covered entity reasonably determines that the breach will not likely result in harm to the affected person and the covered entity must document this determination in writing and keep it for three (3) years.
Notification of Data Subject	Yes, notice must be given to any resident of South Dakota within 60 days of discovery of the breach unless a longer delay is required for a legitimate need of law enforcement. If law enforcement measures require delay, notification must be given within 30 days of the determination that the investigation will not be compromised by notification.
Notification of Government	Yes, if the breach includes more than 250 residents, notification to the attorney general is required.
Notification of Credit Reporting Agencies	Yes, if notification is required to be given to consumers, the person or organization must also notify any consumer credit agencies of the timing, distribution, and content of the notice.
Notification by Third Parties	Yes, covered entities include *any* entities conducting business in the state that licenses personal information.
Timing of Notification	**For data subjects:** within 60 days. **For the government:** No statutorily-designated timeline **For credit reporting agencies:** "without unreasonable delay." *Exception*: Delays are permitted if law enforcement determines that notification would impede a criminal investigation. Notice must then be given within 30 days after it is determined that it would not impede the investigation.
Form of Notification	Notice may be given in writing or electronically, if the person's primary method of communication with the individual is by electronic means. However, if the organization or person demonstrates that the cost of providing notice would exceed $250,000, that the affected class exceeds 500,000 individuals, or that the person

	has insufficient contact information, they may provide substitute notice. Substitute notice requires all of the following: • Providing email notice • Posting a conspicuous notice on the website, and • Notification to major statewide media
Exemptions or Safe Harbors	If a person or organization maintains its own notification procedures pursuant to a security policy that are consistent with the timing requirements of the statute and the subjects are notified in compliance with that policy, they are deemed to be compliant. If a person or organization is regulated by HIPAA or the Gramm-Leach-Bliley Act, and maintains a notification procedure in accordance with the provisions set out by those laws, they are deemed to be in compliance.
Consequences of Non-Compliance	*Government enforcement?* The attorney general may prosecute violations as a deceptive act or practice under South Dakota law. Additionally, outside of the penalties included for deceptive acts, the attorney general may bring an action to recover a civil penalty of not more than $10,000 per day per violation on behalf of the state. The attorney general may recover attorneys' fees for any actions brought in accordance with this chapter. *Private right of action?* No, the statute does not expressly provide for a private right of action.
Credit Monitoring Required	—

TENNESSEE

State and Statute	TN. 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	An individual's first name or initial and last name, in combination with any of the following: • Social Security number • Driver's license number • Account, debit card, or credit card number in combination of any required security code or password that would permit access to an individual's financial account This does not include information that is lawfully made available through public government records or information that has been redacted or otherwise made unusable.
Definition of Breach	The acquisition of unencrypted computerized data, or encrypted computerized data with an encryption key, by an unauthorized person that materially compromises the security, confidentiality, or integrity or personal information maintained by the information holder. This definition does not include good faith acquisition of personal information by an employee or agent for the purposes of the covered entity if the information is not used or subject to further unauthorized disclosure. The definition of "unauthorized user" explicitly includes employees who obtain the personal information with intent to use it for unlawful purposes.
Threshold for Notification	Upon the discovery or notification of a breach, the covered entity must inform any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Notification of Data Subject	Yes, notice must be given to any resident of Tennessee whose information was, or is reasonably believed to have been, acquired by an unauthorized person.

TENNESSEE

Notification of Government	—
Notification of Credit Reporting Agencies	Yes, if more than 1,000 individuals must be notified at one time, the information holder must notify consumer credit reporting agencies and credit bureaus that compile and maintain files on consumers. They must be informed of the timing, distribution, and content of the notices.
Notification by Third Parties	Yes, any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of system security 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 of system security, unless a longer period of time is required due to the legitimate needs of law enforcement.
Timing of Notification	**For data subjects:** Not later than 45 days. **For consumer reporting agencies:** No statutorily mandated deadline. Notification may be delayed if law enforcement determines that it will impede criminal investigations. After law enforcement determines that notification will no longer impede investigations, the notice to individuals must be made within 45 days.
Form of Notification	Notice may be given in writing or electronically, if the primary method of communication with the individual is by electronic means. However, if the information holder demonstrates that the cost of providing notice would exceed $250,000, that the affected class exceeds 500,000 individuals, or that the person or business has insufficient contact information, they may provide substitute notice. Substitute notice consists of all of the following: • Providing email notice • Posting a conspicuous notice on the information holder's website • Notification to major statewide media

TENNESSEE

Exemptions or Safe Harbors	If the covered entity maintains its own notification procedure as a part of an information security policy, the covered entity may notify pursuant to that policy, so long as it complies with the timing requirements of the statute. The statute does not apply to covered entities subject to the Gramm-Leach-Bliley Act of 1999 or HIPAA.
Consequences of Non-Compliance	*Government enforcement?* No. *Private right of action?* Yes. A customer of an information holder who is a business entity, who is injured by a violation of this statute may institute a civil action to recover damages and to enjoin further unlawful action by the information holder. This does not preempt rights of action that a consumer may have under other laws.
Credit Monitoring Required	—

TEXAS

State and Statute	TX. 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	**Personal identifying information** is any information that alone or combined with other information identifies an individual. This explicitly includes, but is not limited to: • Name • Social Security number • Date of Birth • Government-issued identification number • Mother's maiden name • Unique biometric data (fingerprints, voice print, iris or retina image) • Unique electronic identification number, address, or routing code • Telecommunication access devices (any card, plate, code, account number, electronic serial number, etc. that could allow an individual to obtain money, goods, services or things of value or initiate a transfer of funds not by paper instrument. **Sensitive personal information** is any person's first name or initial combined with any one or more of the following (if the name and items are not encrypted): Social Security number, driver's license or government-issued ID number, or account, credit or debit card number in combination with any required security code, access code, or password that would allow access to financial accounts. It also includes information that identifies an individual and relates to the health of an individual, the provisioning of heath care to the individual, or payment for health care. It does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.
Definition of Breach	Any "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data."

TEXAS

	Importantly, the good faith acquisition by an employee or agent of the covered entity for purposes of the covered entity is not a breach unless the person uses or discloses the information in an unauthorized manner.
Threshold for Notification	After discovery of a breach (or reasonable belief that a breach has occurred) of any sensitive information of any individual, including nonresidents.
Notification of Data Subject	Yes, any person whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person must receive a disclosure of that fact without unreasonable delay and not later than 60 days after the breach (unless such notification would impede criminal investigations). If the person whose data is breached is a non-Texas resident and lives in a state that requires notice of breach, that state's notification law may be used instead.
Notification of Government	Yes, the attorney general must be notified as soon as practicable, and not more than 30 days after the breach, if and only if, the breach includes 250 residents of the state.
Notification of Credit Reporting Agencies	Yes, if a person is required to notify 10,0000 people or more at one time, they must notify all consumer reporting agencies. This notification must include the timing, distribution, and content of the notices sent to data subjects. Notification must be sent "without unreasonable delay."
Notification by Third Parties	Yes, any person who maintains computerized data that includes sensitive personal information not owned by the person 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.
Timing of Notification	**For data subject:** "without unreasonable delay" and not more than 60 days after the breach. **For the government:** "as soon as practicable," and not more than 30 days after the breach. **For consumer reporting agencies:** "without unreasonable delay."

TEXAS

Form of Notification	Notice may be given in written form to the last known address of an individual or electronic notice consistent with 15 U.S.C. § 7001. Notification to the attorney general must include a detailed description of the nature and circumstances of the breach or the use of sensitive information as a result of the breach, the number of residents affected, the number of residents who have been sent disclosure, the response measures taken or intended to be taken, and whether law enforcement is investigating the breach. If more than 500,000 people are affected, the cost of giving notice would exceed $250,000, or the covered entity does not have sufficient contact information, notice may be given through email, conspicuous posting of a notice on one's website, or notice published in or broadcast on major, statewide media.
Exemptions or Safe Harbors	If a covered entity has its notification procedures in its information security policy, that form of notification is acceptable, so long as it complies with timing requirements of the statute.
Consequences of Non-Compliance	*Government enforcement?* If a person fails to give timely notice, they will be liable to the state for a civil penalty of $100 per person per day. The suit to recover this amount will be brought by the attorney general. A person who violates this chapter will be liable for at least $2,000, but not more than $50,000. The suit to recover this amount will be brought by the attorney general. The attorney general may bring suit if they believe that a person has engaged in, is engaging in, or is about to engage in conduct violating this chapter. Courts are explicitly granted equitable powers in fashioning remedies. *Private right of action?* No, there is no private right of action.
Credit Monitoring Required	—

US VIRGIN ISLANDS

State and Statute	US Virgin Islands 14 V.I.C. §§ 2209-2212
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	An individual's first name or first initial with an individual's last name combined with any of the following (whether encrypted or unencrypted): • Social Security number • Driver's license number • Account, credit card, or debit card number in combination with any required security code or password that would permit access to an individual's financial account *Exception*: This definition explicitly excludes publicly available information that is lawfully made available through government records.
Definition of Breach	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the covered entity. This definition does not include good faith acquisition of personal information by an employee or agent for the purpose of the covered entity if the information is not used or subject to further unauthorized disclosure.
Threshold for Notification	Following the discovery or notification of a breach, disclosure shall be made to any Virgin Island resident whose unencrypted, personal information was, or is reasonably believed to have been acquired by an unauthorized person.
Notification of Data Subject	Yes, any Virgin Islands resident whose information has been acquired by an unauthorized party must be notified "in the most expedient time possible without unreasonable delay" consistent with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
Notification of Government	—

US VIRGIN ISLANDS

Notification of Credit Reporting Agencies	—
Notification by Third Parties	Yes, any person or business that maintains computerized data that includes personal information that the person or business 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.
Timing of Notification	**For data subjects:** "in the most expedient time possible without unreasonable delay." Notification may be delayed if law enforcement determines that it would impede a criminal investigation.
Form of Notification	Notice may be given in writing or electronically, if the person's primary method of communication with the individual is by electronic means. However, if the covered entity demonstrates that the cost of providing notice would exceed $100,000, that the affected class exceeds 50,000 individuals, or that the covered entity has insufficient contact information, it may provide substitute notice. Substitute notice consists of all of the following: • Providing email notice • Posting a conspicuous notice on the information holder's website • Notification to major territory-wide media
Exemptions or Safe Harbors	If a covered entity maintains its own notification procedures as a part of a security policy that is consistent with the timing requirements of the statute, the covered entity may notify through its procedure and be deemed to be in compliance.
Consequences of Non-Compliance	*Government enforcement?* No. *Private right of action?* Yes, there is a private right of action. Any customer injured may bring a civil action for damages. Any business who has or proposes to violate the statute may be enjoined.

	The statute does not preempt any other rights that a consumer may have under another statute.
Credit Monitoring Required	—

UTAH

State and Statute	UT. 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 first name or initial and last name combined with any of the following data elements relating to that person when either the name or data element is unencrypted or not protected by another method that renders the data unreadable or unusable: • Social Security number • Financial account, debit card, or credit card number and any required security code and password that would provide access to the accounts • Driver's license number or state identification card number *Exception*: This definition explicitly excludes information contained in government records or in widely distributed media lawfully made available to the public.
Definition of Breach	An unauthorized acquisition of computerized data that compromises security, confidentiality, or integrity of personal information. This does not include acquisitions by a person's employee or agent unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.
Threshold for Notification	If there is a breach, the covered entity must conduct a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft. If this investigation reveals that misuse for identity theft has occurred or is reasonably likely to occur, the covered entity must notify all Utah residents who are affected.
Notification of Data Subject	Yes, see "Threshold for Notification" above.

UTAH

Notification of Government	Yes, if the investigation of the breach reveals that 500 or more Utah residents were affected, the covered entity must provide notice to the Office of the Attorney General and the Utah Cyber Security Center. Both of these notifications are considered classified records.
Notification of Credit Reporting Agencies	Yes, if the investigation of the breach reveals that the misuse of personal information relating to 1,000 or more Utah residents, for identity theft or fraud purposes, has occurred or is reasonably likely to occur.
Notification by Third Parties	Yes, a person who maintains computerized data that includes personal information that the person 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 person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur.
Timing of Notification	All notifications must be given "in the most expedient time possible without unreasonable delay" after restoring the reasonable integrity of the system, determining the scope of the breach, and considering the investigative needs of law enforcement. If notification is delayed at the request of a law enforcement agency that determines that notification may impede a criminal investigation, the notification shall be given "without unreasonable delay in the most expedient time possible" after it is determined that it will no longer impede the investigation.
Form of Notification	Notice may be given in writing by first-class mail, electronically if the primary method of communication was by electronic means, or by telephone. If none of the above are "feasible," the person or business may notify consumers by publication in a newspaper of general circulation. A notification to the attorney general or Utah Cyber Center must include: • The date of the breach • The date the breach was discovered • The total number of people affected, including the number of Utah residents affected • The type of personal information involved in the breach • A short description of the breach

Exemptions or Safe Harbors	The statute does not apply to financial institutions as defined by 15 U.S.C. § 6809. If a covered entity maintains its own procedures for notification pursuant to an information security policy, notification under that procedure is deemed to comply so long as it is consistent with the statute's timing requirements, and the covered entity notifies each affected Utah resident in accordance with the covered entity's information security policy in the event of a breach. If a covered entity is regulated by state or federal law and maintains procedures for a breach under applicable law established by the primary state or federal regulator, it is considered to be in compliance if the covered entity notifies each affected Utah resident in accordance with the other applicable law in the event of a breach.
Consequences of Non-Compliance	*Government enforcement?* The attorney general may impose civil penalties of up to $2,500, for a violation (or series of violations) regarding one consumer, but no more than $100,000, in the aggregate for related violations unless 10,000 or more Utah residents are affected and 10,000 or more non-Utah residents are affected, or the parties settle for a greater amount. The attorney general may also seek injunctive relief and attorney fees. An administrative action must be commenced no later than 10 years after the day on which the alleged breach last occurred, and a civil action must be commenced no later than five (5) years after such date. The attorney general has the power to subpoena, compel production, and conduct investigations. *Private right of action?* No, there is no private right of action.
Credit Monitoring Required	—

VERMONT

State and Statute	VT. 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	Personally identifiable information means a person's first name or initial and last name combined with one or more of the following data elements when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons: • Social Security number • Driver's license number, nondriver state identification card number, individual taxpayer identification number, passport number, military identification card number, or any other identification number issued by the government • Financial account, credit card, or debit card number if the number could be used without an access code or password • Passwords, personal identification number, or other access codes for a financial account • Unique biometric data generated from technical analysis of the human body • Genetic information • Health records of a wellness program, a healthcare professional's medical diagnosis or treatment of a consumer, or a health insurance policy number *Exception*: This definition explicitly excludes publicly available information that is lawfully made available through government records.

VERMONT

Definition of Breach	Unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials (i.e., a consumer's user name or email address, in combination with a password or an answer to a security question, that together permit access to an online account) maintained by a data collector. A security breach does not include good faith, but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, as long as the information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure. In determining whether a breach has or is reasonably like to have occurred, a data collector shall consider: • Indications that the information is in the physical possession of an unauthorized party • Indications that the information has been downloaded or copied • Indications that the information was used by an unauthorized party • Whether the information has been made public
Threshold for Notification	Notification is required upon breach, unless it is determined that misuse of personal information or login credentials is not reasonably possible after a breach. In such a case, the breach must only be reported to the attorney general and Department of Finance Regulation, and can be made a trade secret thereafter.
Notification of Data Subject	Yes, notification must be given to the data subject "in the most expedient time possible and without unreasonable delay, but not later than 45 days after discovery."
Notification of Government	Yes, notice (including a preliminary description of the breach) shall be given to the attorney general "within 14 business days" of the data collector's discovery of the breach or when the data collector provides notification to consumers, whichever is sooner. This notice should include how many Vermont residents were affected and a copy of the consumer notification (with personal information redacted). If the breach is limited to log in credentials, the data collector is only required to notify the attorney general and/or Department

	of Finance Regulation if the login credentials were acquired directly from the data collector or their agent. If a data collector is regulated by the Department of Financial Regulation, they must provide the department notice alongside the attorney general. If it is determined that misuse of personal information or login credentials is not reasonably possible after a breach, though relieved from notifying the consumers, the data collector must provide the Vermont Attorney General and the Department of Finance Regulation with a detailed explanation of the determination. This notice may be designated as a trade secret. A data collector who, prior to the date of the breach, on a form and in a manner prescribed by the attorney general, had sworn in writing to the attorney general that it maintains written policies and procedures to maintain the security of personally identifiable information or login credentials and responds to a breach in a manner consistent with Vermont law shall notify the attorney general of the date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers.
Notification of Credit Reporting Agencies	Yes, if 1,000 people must be notified at one time, the data collector shall notify all consumer reporting agencies of the timing, distribution, and content of the notices "without unreasonable delay."
Notification by Third Parties	—
Timing of Notification	**For data subjects:** "in the most expedient time possible and without unreasonable delay, but not later than 45 days after discovery." **For the government:** "within 14 business days" of the data collector's discovery of the breach or when the data collector provides notification to consumers, whichever is sooner. **For consumer reporting agencies:** "without unreasonable delay." The consumer notice may be further delayed if law enforcement determines that notification would jeopardize an investigation, national or homeland security, or public health. If this request for delay is not made in writing by law enforcement, the entity must document it in writing. Once the

	law enforcement agency informs the entity in writing that the delay is no longer needed, notification must be given "without unreasonable delay."
Form of Notification	Notice may be given in writing, telephonically, or electronically (if this is the primary means of communication, the electronic notice does not contain a hyperlink asking for more personal information, and conspicuously warns the person not to provide personal information in response to communications regarding security breaches). The notice to the consumer shall include all of the following if known by the data collector: • The incident in general terms • The type of personally identifiable information that was subject to the breach • The general acts of the data collector to protect the information from further breach • A telephone number (toll-free if available) that the customer may call for further information or assistance • Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports • The approximate date of the security breach If the security breach is limited to login credentials of an online account, other than an email, notice must be given advising the consumer to take steps necessary to protect the account. If the security breach is limited to an unauthorized acquisition of login credentials for an email account, notice may not be provided via email, and the data collector must provide notice through another method or through the email account when the user is connected at an IP address that the data collector knows to be customarily used by the consumer. Substitute notice may be made if the data collector demonstrates that the cost of providing notification in the above manner would exceed $10,000 or the data collector does not have sufficient contact information. Substitute notice requires conspicuous posting of notice on the data collector's website if they maintain one and notification on major statewide and regional media.
Exemptions or Safe Harbors	If the company is subject to HIPAA, it is deemed compliant if: the data collector experiences a security breach that requires notification under HIPAA and is limited to health

	records, records of a wellness program, health care professional's medical diagnosis or treatment of the consumer, or the health insurance policy number of the consumer. Any financial institution governed by the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice or Final Guidance on response Programs for Unauthorized Access to Member Information and Member Notice is exempt. Still, a financial institution that falls under these exceptions must provide notice to the Department of Financial Regulation "as soon as possible" after becoming aware of a breach.
Consequences of Non-Compliance	*Government enforcement?* Yes, the attorney general and Department of Financial Regulation have sole enforcement authority. *Private right of action?* No, there is no private right of action.
Credit Monitoring Required	—

VIRGINIA

State and Statute	VA. 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 nonprofit legal entity.
Definition of Personal Information	Personal information means the first name or initial and the last name of an individual combined with any of the following in their non-encrypted and unredacted form: • Social Security number • Driver's license number • Financial account, debit card, or credit card number, in combination with any security code/passcode that would permit access to an individual's financial accounts • Passport number • Military ID number The term does not include information that is lawfully obtained from a publicly available source or from government records made available to the public. "Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information: • Five digits of a Social Security number; or • The last four digits of a driver's license number, state identification card number, or account number
Definition of Breach	Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth.

VIRGINIA

Threshold for Notification	If there is a breach of personal information belonging to any Virginia resident, they must be notified "without unreasonable delay."
Notification of Data Subject	Yes, if any resident's personal information is subject to a breach, the entity or person who owns or licenses that information must notify the affected individual without unreasonable delay.
Notification of Government	Yes, if any resident's personal information is subject to a breach, the entity or person who owns or licenses that information must notify the Office of the Attorney General of the breach. If more than 1,000 people must be notified as a result of a breach, the attorney general must be notified of the timing, distribution, and content of notices to consumers "without unreasonable delay." Additionally, notwithstanding any other provision, any employer or payroll service provider that maintains computerized data related to income tax withholding shall notify the attorney general "without unreasonable delay" if taxpayer identification numbers, in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and 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. This notification must include the name and federal identification number.
Notification of Credit Reporting Agencies	Yes, if more than 1,000 people must be notified as a result of a breach, all consumer reporting agencies must be notified of the timing, distribution, and content of notices to consumers "without unreasonable delay."
Notification by Third Parties	Yes, an individual or entity that maintains computerized data that includes personal information that the individual or 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 individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person.

VIRGINIA

Timing of Notification	The data subject, government, and consumer reporting agencies must be notified "without unreasonable delay." However, notice under this provision may be reasonably delayed to allow the individual or entity to determine the scope of the breach and restore reasonable integrity of the system. Notice may also be delayed if, after law enforcement is notified, they determine and advise that the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. Following clearance from law enforcement, notice must be given without unreasonable delay.
Form of Notification	Notice is required to include: • The incident in general terms • The type of personal information that was subject to the breach • The general acts of the individual or entity to protect from further unauthorized access of personal information • The telephone number that a person may call for further information or assistance, if one exists • Advice that directs the person to remain vigilant by reviewing account statements and free credit reports Notice may be provided by telephone, in writing, or electronically. If the entity demonstrates that the cost of providing notice through the above methods would cost over $50,000, that the affected class of Virginia residents would be more than 100,000, or the individual or entity does not have sufficient contact information or consent to provide notice in the above manners, it may provide substitute notice. Substitute notice consists of all of the following: • Email notice, if they have the email addresses of the affected class • Conspicuous posting of notice on the website, if they maintain one • Notice to all major statewide media

Exemptions or Safe Harbors	If an entity maintains its own notification procedure, it may utilize that procedure to satisfy this provision so long as it complies with the timing requirements of the statute. Any entity that is governed by, and abides by, Title V of the Gramm-Leach-Bliley Act and maintains procedures compliant with that Act is deemed to be in compliance with this provision. If an entity complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator is in compliance with this provision. The statute does not apply to any entity regulated by the State's Corporation Commission's Bureau of Insurance. The statute does not apply to criminal intelligence systems that are maintained by law enforcement agencies and the organized Criminal Gang File of the Virginia Criminal Information Network.
Consequences of Non-Compliance	*Government enforcement?* The Office of the Attorney General may enforce through civil action. However, if the violation is committed by a state-chartered or licensed financial institution, the only party that may enforce these provisions is the institution's primary state regulator. The attorney general may impose a civil penalty not to exceed $150,000 per breach or series of breaches of a similar nature that are discovered in a single investigation. *Private right of action?* Yes, the statute states that nothing in the statute prevents the individual from recovering direct economic damages.
Credit Monitoring Required	—

WASHINGTON

State and Statute	Washington Rev. Code § 19.255.010 et seq.
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	Personal information means an individual's first name or first initial and last name in combination with any one or more of the following: • Social Security number • Driver's license number or Washington identification card number • Account, credit card, or debit card number in combination with any required password or security/access code that would permit access to the individual's financial account, or any other numbers or information that can be used to access a person's financial account • Full date of birth • Private key that is unique to an individual and 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 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 fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. Personal information also includes a user name and email address in combination with a password or security questions and answers that would permit access to an online account. Additionally, if there is not a name combined with the information, it is still personal information if: • It is not encrypted, redacted, or otherwise rendered unusable

	• It would enable a person to commit identify theft against a consumer *Exception*: 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	Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business. This explicitly does not include good faith acquisitions of personal information by an employee or agent of the person or business for the purposes of the person or business so long as it is not used or subject to further unauthorized disclosure.
Threshold for Notification	Any person or business that conducts business in the state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.
Notification of Data Subject	Yes, see “Threshold for Notification” above.
Notification of Government	Yes, if 500 Washington residents must be notified as a result of a single breach, the entity must notify the attorney general within 30 days of the breach. That notification must include: • The number of Washington residents included (or an estimate thereof, if the exact number is not known) • A list of the types of personal information that was reasonably believed to have been subject to the breach • The time frame of the exposure, if known including the date of the breach and the date of the discovery thereof • A summary of the steps taken to contain the breach

	• A single sample copy of the security breach notification, excluding any personal information If any information relevant to this notification is later discovered after the attorney general is given the notification, the notification must be updated.
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Yes, any person or business that maintains or possesses data that may include personal information that the person or business does not own or license 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.
Timing of Notification	**For data subjects:** "in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered." **For the government:** "within 30 days of the breach." Notification to individuals may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation.
Form of Notification	Notification may be written or electronic. If the cost of providing notice in either of these ways would cost more than $250,000, there are more than 500,000 residents affected, or the entity does not have the requisite information to provide notice in this manner, it may provide substitute notice. Substitute notice shall consist of all of the following: • Email notice, when the entity has the email address for the subject person • Conspicuous posting of notice on the entity's website if they maintain one • Notification to major statewide media If the breach only includes a username or password, notice may be provided by email in the first instance, but that notification must additionally prompt the subject to change their password or security questions. However, if the breach includes the login credentials of an email account furnished by

	the business, it must use one of the above notification methods and prompt the user to change their password or security information.
	
	Notification given pursuant to this statute must:
	• Be written in plain language
	• Include:
	  ○ The types of personal information accessed
	  ○ The name and contact of the person or entity who experienced the breach
	  ○ A timeframe of the exposure (including the date of the breach and its discovery)
	  ○ The toll-free telephone numbers and addresses of the major credit reporting agencies

Exemptions or Safe Harbors	If a company maintains its own breach notification policy that is consistent with the timing requirements of the statute, notification in accordance with that procedure is deemed compliant. If a company is regulated by HIPAA and complies with the notification requirements thereunder, it is deemed compliant. If a financial institution is under the authority of the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, or the Federal Reserve System, it is deemed to be compliant if it provides notice to affected consumers pursuant to interagency guidelines. Still, it must inform the attorney general and its primary federal regulator.
Consequences of Non-Compliance	*Government enforcement?* Violation of the statute may be enforced by the attorney general as an unfair or deceptive act. Civil penalties can be up to $7,500 per violation, as well as an injunction. *Private right of action?* Yes, if the consumer is injured by a violation.
Credit Monitoring Required	—

WEST VIRGINIA

State and Statute	W. VA. 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 initial and last name combined with any of the following in its unredacted or unencrypted form: • A Social Security number • A driver's license number or state identification card number issued in lieu of a driver's license • A financial account, debit card, or credit card number in combination with any required security code that would permit access to a resident's financial accounts This definition does not include information that is lawfully obtained from publicly available government records. In order for a piece of information to be deemed "redacted," it must include no more than four digits of a Social Security number, driver's license number, state identification card number, or account number.
Definition of Breach	Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident.
Threshold for Notification	An individual or entity that owns or licenses computerized data that includes personal information shall give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system.

WEST VIRGINIA

Notification of Data Subject	Yes, a data subject must be given notice without unreasonable delay if a breach occurs.
Notification of Government	—
Notification of Credit Reporting Agencies	Yes, if more than 1,000 individuals must be notified of a breach, the entity must notify all consumer reporting agencies without unreasonable delay. The covered entity is not required to provide the names or other personal information of breach notice recipients.
Notification by Third Parties	Yes, an individual or entity that maintains computerized data that includes personal information that the individual or 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.
Timing of Notification	All notification under this provision must be made "without unreasonable delay" with the exception of notification given from a non-owner of information to an owner of information when the non-owner experiences a breach. This must be done "as soon as practicable." Notification may be delayed if law enforcement determines that the notice will impede a criminal or civil investigation or homeland or national security. Notification must be given without unreasonable delay after law enforcement determines that the notification will no longer impede the investigation or threaten security.
Form of Notification	Notice may be written, telephonic, or electronic. If the entity or individual demonstrates that providing notice in this manner will cost more than $50,000, that the affected class exceeds 100,000 people, or that it does not have sufficient contact information to provide this notice, it may give substitute notice. Substitute notice requires two of the following: • Email notice • Conspicuous posting on the entity's website • Notice to major state-wide media The notice given must include: • A description of the information subject to the breach

	• A telephone number or website address that the individual may use to contact the entity or the agent of the entity to learn the type of information that the entity maintains and whether the entity maintained information about that individual • The toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a security freeze or fraud alert.
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 and that are consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if it notifies residents of West Virginia in accordance with its procedures in the event of a breach of security of the system. If a financial institution is in compliance with notification guidelines prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Gramm-Leach-Bliley Act, it is deemed compliant with this article. If an entity complies with the notification procedures and requirements of its primary or functional regulator, it is deemed compliant with the statute.
Consequences of Non-Compliance	*Government enforcement?* Yes, by the attorney general. In order for a civil penalty to be enforced, there must be a court finding of "repeated and willful" violations. The maximum civil penalty may not exceed $150,000 per breach or series of breaches of a similar nature under a single investigation. If a licensed financial institution violates the statute, action may only be brought by a financial institution's primary functional regulator. *Private right of action?* No, there is no private right of action.
Credit Monitoring Required	—

WISCONSIN

State and Statute	WI. 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 initial and last name of an individual in combination with any of the following so long as they are not publicly available information, redacted, or altered in a way that renders them unreadable: • Social Security number • Driver's license or state identification number • Financial account credit card, or debit card number or any security code or password thereto • DNA profile as defined in 939.74(2d)(a) • Unique biometric data including fingerprint, voice print, retina or iris image, or any other unique physical representation Publicly available information is any information made lawfully available through any media or government records or disclosures.
Definition of Breach	Knowledge that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information.

WISCONSIN

Threshold for Notification	Notification must be made if an entity knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized, unless the acquisition does not create a material risk of identity theft or the information was acquired in good faith by an employee or agent and used for a lawful purpose of the entity. If an entity whose principal place of business is not located in Wisconsin knows that personal information pertaining to a resident of Wisconsin 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 Wisconsin who is the subject of the personal information.
Notification of Data Subject	Yes, a data subject must be given notice "within a reasonable time," not to exceed 45 days after the entity learns of the breach.
Notification of Government	—
Notification of Credit Reporting Agencies	Yes, if more than 1,000 people must be notified as a result of a breach, all consumer reporting agencies must be notified "without unreasonable delay" of the timing distribution, and content of the notices.
Notification by Third Parties	Yes, 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 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.
Timing of Notification	**For data subjects:** "within a reasonable time," not to exceed 45 days from the time the entity learned of the acquisition. **For consumer reporting agencies:** "without unreasonable delay." "Reasonableness" determinations will explicitly take into account the number of individuals who need to be notified and the methods of communication available.

WISCONSIN

	Notification may be delayed if law enforcement asks an entity not to provide notice in order to protect an investigation or homeland security. If such a request is made, an entity may not make any notification or publication of the breach.
Form of Notification	Notice may be given by mail or another method that the entity has previously employed to communicate with the subject. If the entity does not have, and after reasonable diligence cannot determine, the mailing address of the subject nor has it communicated with the subject, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject. The notice must indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident receiving the notification. Upon request by the data subject notified under this provision, the entity must notify the subject of the personal information that was acquired.
Exemptions or Safe Harbors	If an entity is subject to and in compliance with the requirement of HIPAA or the Gramm-Leach-Bliley Act, it is exempt from this provision.
Consequences of Non-Compliance	*Government enforcement?* No. *Private right of action?* Failure to comply with the statute is not necessarily negligent or a breach of any duty, but may be evidence of negligence or a breach of legal duty.
Credit Monitoring Required	—

WYOMING

State and Statute	WY. 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 initial and last name of a person in combination with the following unredacted data elements: • Social Security number • Driver's license number • Account, credit card, or debit card number in combination with any security code or password that would allow access to the financial account of a person • Tribal identification card • Federal or state government-issued identification card • Shared secrets or security tokens that are known to be used for database authentication • Username or email address in combination with a password or security questions and answers that would permit access to an online account • Birth or marriage certificate • Medical information (meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional) • Health insurance identification (meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person, or information related to a person's application and claims history) • Unique biometric data (meaning data generated from measurements or analysis of human body characteristics for authentication purposes • Individual taxpayer identification number This definition does not include information, regardless of source, contained in government records or widely distributed media made lawfully available to the public.

WYOMING

Definition of Breach	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal identifying information maintained by a person or business or is reasonably believed to cause injury to a Wyoming resident. This definition excludes the good faith acquisition of information by an employee or agent for the purposes of the covered entity provided that the information is not used or subject to further unauthorized disclosure.
Threshold for Notification	When an entity becomes aware of a security breach of the system, it must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has or will be misused. If the investigation leads to the conclusion that the misuse has occurred or is reasonably likely to occur, the entity shall give notice.
Notification of Data Subject	Yes, notification must be given "as soon as possible" and "in the most expedient time possible and without unreasonable delay" consistent with law enforcement needs and any measures necessary to determine the scope of the breach and restore the system's integrity.
Notification of Government	—
Notification of Credit Reporting Agencies	—
Notification by Third Parties	Yes, any person who maintains computerized data that includes personal identifying information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable following the determination that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.
Timing of Notification	**For the data subject:** "as soon as possible" and "in the most expedient time possible and without unreasonable delay." This may be delayed to determine the scope of the breach or to restore the system's integrity. Notification may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation.

WYOMING

Form of Notification	Notification may be written or electronic. Substitute notice may be given if the covered entity demonstrates: • The cost of providing notice would exceed $10,000 for Wyoming-based persons or businesses and $500,000 for all other businesses operating but not based in Wyoming • The affected class that must be notified is more than 10,000 for a Wyoming-based company and 500,000 for all other businesses operating but not based in Wyoming • The entity does not have sufficient contact information Substitute notice shall include all of the following: • Conspicuous posting of the notice on the internet, the world wide web, or a similar electronic carrier electronic system site of the entity, if they maintain one • Notification to major state-wide media (including a toll-free phone number where an individual can learn whether or not that individual's personal data was included in a security breach) Notice shall be clear and conspicuous and shall include: • A toll-free number that the individual may use to contact the person collecting the data or his agent and from which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies • The types of personal identifying 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 reasonably possible to determine • In general terms, the actions taken by the entity to protect the system from further breaches • Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports • Whether notification was delayed as a result of a law enforcement investigation, if reasonably possible to determine at the time notice is provided
Exemptions or Safe Harbors	A covered entity under HIPAA that complies with the provisions of HIPAA is deemed compliant with the statute. Any financial institution or credit union that maintains notification procedures subject to the Gramm-Leach-Bliley Act is deemed compliant with the statute if the financial institution notifies affected Wyoming residents in compliance with that Act.

WYOMING

Consequences of Non-Compliance	*Government enforcement?* The attorney general may bring an action in law or equity to address any violation of this statute and for other relief that may be appropriate to ensure proper compliance with this statute, to recover damages, or both. *Private right of action?* No.
Credit Monitoring Required	—

This report is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. Scott W. Pink, an O'Melveny special counsel licensed to practice law in California and Illinois; Randall W. Edwards, an O'Melveny partner licensed to practice law in California; Sid Mody, an O'Melveny partner licensed to practice law in Texas; Emily Losi, an O'Melveny associate licensed to practice law in New York; Ashley Kang, an O'Melveny summer law clerk; Sean Oh, an O'Melveny summer law clerk; and Gavin Reece Barrett, an O'Melveny summer law clerk; contributed to the content of this newsletter. The views expressed in this newsletter are the views of the authors except as otherwise noted.

O'Melveny

Austin • Beijing • Brussels • Century City • Dallas • Hong Kong • Houston • London • Los Angeles • New York
Newport Beach • San Francisco • Seoul • Shanghai • Silicon Valley • Singapore • Tokyo • Washington, DC
omm.com