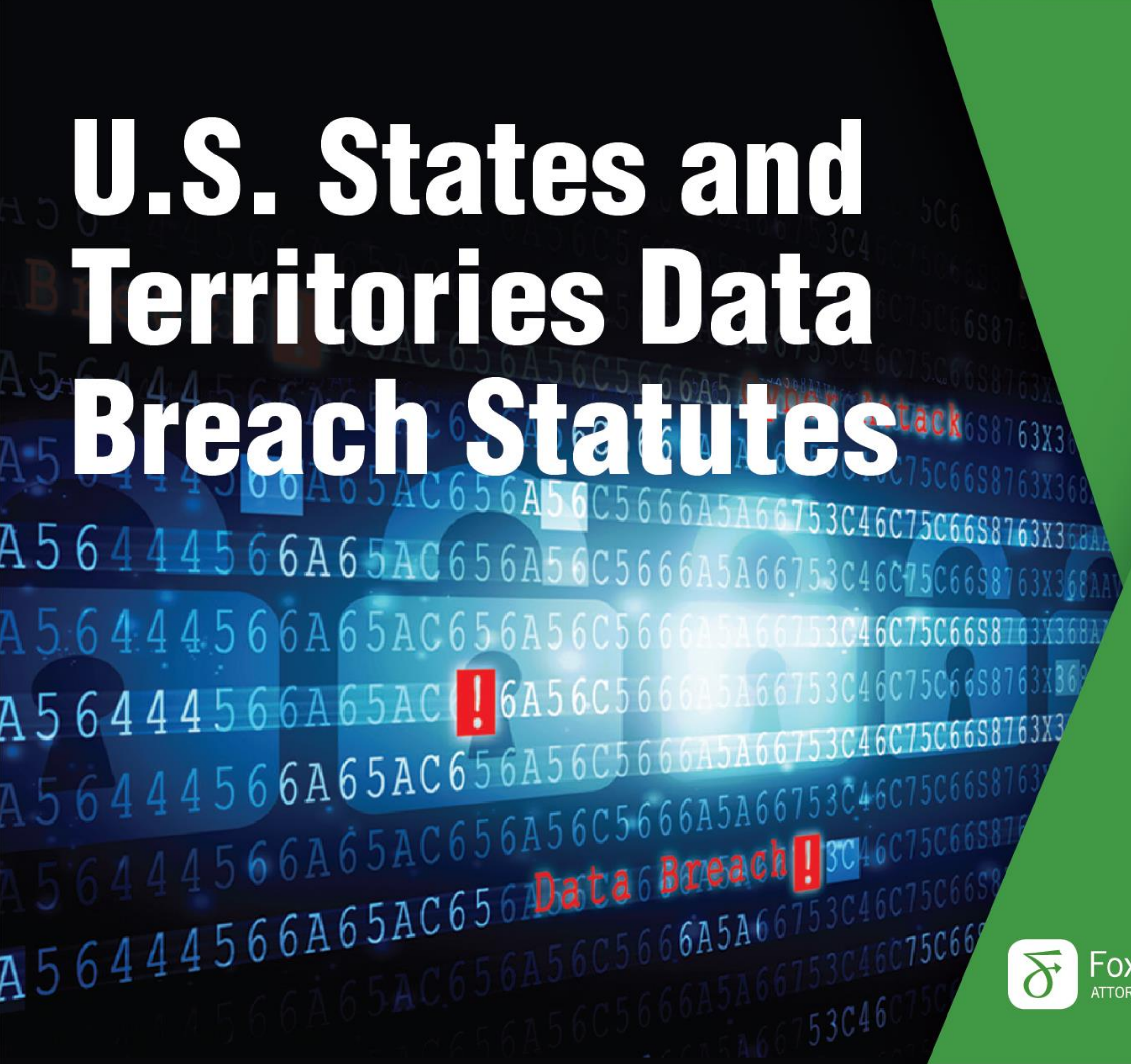
U.S. States and Territories Data Breach Statutes



Fox Rothschild LLP
ATTORNEYS AT LAW

Fox Rothschild's Privacy and Data Security practice group maintains this searchable PDF document to inform businesses of the breach notification statutes in each of the 50 states, Guam, Puerto Rico and the U.S. Virgin Islands, so they can better understand their rights, obligations and potential liability.

If you have any questions regarding data breach notifications, please contact one of the members of Fox Rothschild's Privacy & Data Security practice who advise companies on these requirements and are poised to help you respond swiftly and decisively should a breach occur.

Visit the **Privacy & Data Security** practice on Fox Rothschild's website for more information and additional client resources.

General Breach Contacts

Mark G. McCreary | 215.299.2010
Co-Chair, Privacy & Data Security
mmccreary@foxrothschild.com

Ryan T. Becker | 215.299.2033
Partner
rbecker@foxrothschild.com

Kristen W. Broz | 202.794.1220
Counsel
kbroz@foxrothschild.com

Christopher J. Pippett | 610.458.6703
Partner
cpippett@foxrothschild.com

Marc C. Tucker | 919.755.8713
Partner
mtucker@foxrothschild.com

Nathanael F. Williams | 610.458.3123
Associate
nfwilliams@foxrothschild.com

HIPAA Breach Contacts

Elizabeth G. Litten | 609.895.3320
Partner and HIPAA Privacy & Security Officer
elitten@foxrothschild.com

Edward J. Cyran | 610.458.4963
Partner
ecyran@foxrothschild.com

Michael J. Kline | 609.895.6635
Partner and Assistant General Counsel
mkline@foxrothschild.com

William H. Maruca | 412.394.5575
Partner
wmaruca@foxrothschild.com

Maureen Demarest Murray | 336.378.5258
Partner
mmurray@foxrothschild.com

Jessica Forbes Olson | 612.607.7478
Partner
jforbesolson@foxrothschild.com

U.S. STATES AND TERRITORIES DATA BREACH STATUTES

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
Utah
Vermont
Virginia
Virgin Islands
Washington
West Virginia
Wisconsin
Wyoming

This chart is current as of June 25, 2021 and should be used for informational purposes only.

State/Territory	**ALABAMA**
Statute	Ala. Stat. § 8-38-1, *et seq.*
Definition of “Personal Information”	Sensitive Personally Identifying Information: An Alabama resident's first name or first initial and last name in combination with one or more of the following; (1) a non-truncated Social Security number or tax identification number; (2) a non-truncated driver’s license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual; (3) a financial account number, including a bank account number, credit card number, or 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 to conduct a transaction that will credit or debit the financial account; (4) any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (5) an individual’s health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or (6) a username or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information. Ala. Stat. § 8-38-2(6) (a).
Definition of “Breach”	“Breach of Security” or “Breach” is defined as the unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach. The term does not include the following: (1) good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity unless the information is used for a purpose unrelated to the business or subject to further unauthorized use; (2) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements; (3) any lawful investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state. Ala. Stat. § 8-38-2 (1).
Analysis of Risk of Harm	If a covered entity 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, the covered entity shall conduct a good faith and prompt investigation. Ala. Stat. § 8-38-4 (a). In determining whether sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an authorized person without valid authorization, the following factors may be considered: (1) indications that the information is in the physical possession and control of a person without valid authorization; (2) indications that the information has been downloaded or copied; (3) indications that the information was used by an unauthorized person; (4) whether the information has been made public. Ala. Stat. § 8-38-4 (b).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The term “Sensitive Personally Identifying Information” does not include information that is truncated, 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, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information. Ala. Stat. § 8-38-2 (b) (2).

Unauthorized Employee Disclosure	Government entities shall be subject to the notice requirements of this chapter. A government entity that acquires and maintains sensitive personally identifying information from a government employer, and which is required to provide notice to any individual under this chapter, must also notify the employing government entity of any individual to whom the information relates. Ala. Stat. § 8-38-9 (a)(5). All government entities are exempt from any civil penalty authorized by this chapter; provided, however, the Attorney General may bring an action against any state, county, or municipal official or employee, in his or her official capacity, who is subject to this chapter for any of the following: To compel the performance of his or her duties under this chapter; To compel the performance of his or her ministerial acts under this chapter; To enjoin him or her from acting in bad faith, fraudulently, beyond his or her authority, or under mistaken interpretation of the law. Ala. Stat. § 8-38-9 (a)(6).
Notification Obligation	Notification is required if sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person who is reasonably likely to cause substantial harm to the individuals to whom the information relates. Ala. Stat. § 8-38-5 (a). If a covered entity determines that notice is not required, the entity shall document the determination in writing and maintain records concerning the determination for no less than five years. Ala. Stat. § 8-38-5 (f).
Notification to Consumer Reporting Agencies	If the number of affected individuals exceeds 1,000, the Entity must notify all consumer reporting agencies without unreasonable delay once it is determined that a breach has occurred and is reasonably likely to cause substantial harm to affected individuals. Ala. Stat. § 8-38-7.
Notification to Regulators	If the number of affected individuals exceeds 1,000, the Entity must notify the Attorney General as expeditiously as possible and without unreasonable delay, and within 45 days once it is determined that a breach has occurred and is reasonably likely to cause substantial harm to affected individuals. Ala. Stat. § 8-38-6 (a).
Notification for Third-Party Data	In the event a third-party agent has experienced a breach of security in the system maintained by the agent, 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. After receiving notice from a third-party agent, a covered entity shall provide notices required under Sections 8-38-5 and 8-38-6. A third-party agent, in cooperation with a covered entity, shall provide information in the possession of the third-party agent so that the covered entity can comply with its notice requirements. A covered entity may enter into a contractual agreement with a third-party agent whereby the third-party agent agrees to handle notifications required under this chapter. Ala. Stat. § 8-38-8.
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. Additionally, 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. Ala. Stat. § 8-38-5 (b). If a federal or state law enforcement agency determines that notice to individuals required under this section would interfere with a criminal investigation or national security, the notice shall be delayed upon the receipt of written request of the law enforcement agency for a period that the law enforcement agency determines is necessary. Ala. Stat. § 8-38-5 (c).
Private Cause of Action /	A violation of the notification provisions of this chapter is an unlawful trade practice under the Alabama Deceptive Trade Practices Act, but does not constitute a criminal offense under Section 8-19-12. A violation of this chapter does not establish a private cause of action under Section 8-19-10. Ala. Stat. § 8-38-9 (a).

Enforcement / Penalties	Notwithstanding any remedy available under subdivision (2) of subsection (a), a covered entity that violates the notification provisions of this chapter 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 chapter. Ala. Stat. § 8-38-9 (b)(1).
Exceptions	Information marked as confidential that is obtained by the Attorney General under Ala. Stat. § 8-38-6 is not subject to any open records, freedom of information, or other public record disclosure law. Ala. Stat. § 8-38-6 (d). It is not a violation of this chapter to refrain from providing any notice required under this chapter if a court of competent jurisdiction has directed otherwise. Ala. Stat. § 8-38-9 (b)(3). All government entities are exempt from any civil penalty authorized by this chapter; provided, however, the Attorney General may bring an action against any state, county, or municipal official or employee, in his or her official capacity, who is subject to this chapter. Ala. Stat. § 8-38-9 (b)(6). An entity subject to or regulated by federal or state laws, rules, regulations, procedures, or guidance on data breach notification established or enforced by the federal or state government is exempt from this chapter as long as the entity does all of the following: (1) maintains procedures pursuant to those laws, rules, regulations, procedures, or guidance; (2) provides notice to affected individuals pursuant to those laws, rules, regulations, procedures, or guidance; (3) timely provides a copy of the notice to the Attorney General when the number of individuals the entity notified exceeds 1,000. Ala. Stat. § 8-38-11; Ala. Stat. § 8-38-12.
Other Key Provisions	The Attorney General shall have the exclusive authority to bring an action for civil penalties. Ala. Stat. § 8-38-9 (a).

State/Territory	**ALASKA**
Statute	Alaska Stat. Ann. § 45.48.010 (West 2019), *et seq.*
Definition of “Personal Information”	“Personal Information” means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of: (A) an individual’s name; and (B) one or more of the following information elements: (i) the individual’s social security number; (ii) the individual’s driver’s license number or state identification card number; (iii) except as provided in (iv) of this subparagraph, the individual's account number, credit card number, or debit card number; (iv) if an account can only be accessed with a personal code, the number in (iii) of this subparagraph and the personal code; or (v) passwords, personal identification numbers, or other access codes for financial accounts. AS § 45.48.090 (7).
Definition of “Breach”	“Breach of the security” means 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; in this paragraph, “acquisition” includes acquisition by: (A) photocopying, facsimile, or other paper-based method; (B) a device, including a computer, that can read, write, or store information that is represented in numerical form; or (C) a method not identified by (A) or (B) of this paragraph. AS § 45.48.090 (1)(A)-(C).
Analysis of Risk of Harm	Disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing, and the documentation shall be maintained for five years. The notification required by this subsection may not be considered a public record open to inspection by the public. AS § 45.48.010 (c).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	A person may not require an individual to transmit the individual’s social security number to access an Internet website unless a password, a unique personal identification number, or another authentication device is also required to access the website. AS § 45.48.400 (a)(3).
Unauthorized Employee Disclosure	Notwithstanding the other provisions of AS 45.48.400 - 45.48.480, a person may disclose an individual's social security number to an employee or agent of the person for a legitimate purpose established by and as directed by the person, but the employee or agent may not use the social security number for another purpose or make an unauthorized disclosure of the individual's personal information. AS § 45.48.450 (a).
Notification Obligation	If a breach of the security of an information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach. AS § 45.48.010 (a).
Notification to Consumer Reporting Agencies	If an information collector is required by AS 45.48.010 to notify more than 1,000 state residents of a breach, the information collector shall also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to state residents. AS § 45.48.040 (a). Information collector who is subject to the Gramm-Leach-Bliley Financial Modernization Act does not need to notify consumer credit reporting agencies. Alaska Stat. § 45.48.040 (c).

Notification to Regulators	N/A
Notification for Third-Party Data	N/A
Timing of Notification	The information collector shall disclose the breach to the state resident in the most expeditious time possible and without unreasonable delay. AS § 45.48.010 (b).
Private Cause of Action / Enforcement / Penalties	If an information collector who is not a governmental agency violates AS 45.48.010--45.48.090 with regard to the personal information of a state resident, the violation is an unfair or deceptive act or practice under AS 45.50.471--45.50.561. However, (1) the information collector is not subject to the civil penalties imposed under AS 45.50.551 but is liable to the state for a civil penalty of up to $500 for each state resident who was not notified under AS 45.48.010--45.48.090, except that the total civil penalty may not exceed $50,000; and (2) damages that may be awarded against the information collector under (A) AS 45.50.531 are limited to actual economic damages that do not exceed $500; and (B) AS 45.50.537 are limited to actual economic damages. AS § 45.48.080 (b). The Department of Administration may enforce (a) of this section against a governmental agency. Alaska Stat. § 45.48.080(c).
Exceptions	An information collector may delay disclosing the breach under AS 45.48.010 if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. However, the information collector shall disclose the breach to the state resident in the most expeditious time possible and without unreasonable delay after the law enforcement agency informs the information collector in writing that disclosure of the breach will no longer interfere with the investigation. AS § 45.48.020.
Other Key Provisions	N/A

State/Territory	**ARIZONA**
Statute	Ariz. Rev. Stat. Ann. § 18-551 (2018), *et seq.*
Definition of “Personal Information”	“Personal Information” means any of the following: (i) An individual's first name or first initial and last name in combination with one or more specified data elements, such as: (ii) An individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account. “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. A.R.S. § 18-551 (7).
Definition of “Breach”	“Breach” or “security system breach” means an unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and un-redacted computerized personal information maintained as part of a database of personal information regarding multiple individuals. A.R.S. § 18-551 (1)(a).
Analysis of Risk of Harm	If a person that conducts business in this state and that owns, maintains or licenses unencrypted and un-redacted computerized personal information becomes aware of a security incident, the person shall conduct an investigation to promptly determine whether there has been a security system breach. A.R.S. § 18-552 (A). In this context, a security incident means an event that creates reasonable suspicion that a person's information systems or computerized data may have been compromised or that measures put in place to protect the person's information systems or computerized data may have failed. A.R.S. § 18-551 (10).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	N/A
Unauthorized Employee Disclosure	“Breach” or “security system breach”: (b) Does not include a Good faith acquisition of personal information by a person’s employee or agent for the purposes of the person if the personal information is not used for a purpose unrelated to the person and is not subject to further unauthorized disclosure. A.R.S. § 18-551 (1)(b).
Notification Obligation	If the investigation results in a determination that there has been a security system breach, the person that owns or licenses the computerized data, within forty-five days after the determination, shall notify the individuals affected pursuant to subsection E of this section and subject to the needs of law enforcement as provided in subsection D. A.R.S. § 18-552 (B)(1).
Notification to Consumer Reporting Agencies	If the breach requires notification of more than one thousand individuals, notify both: the three largest nationwide consumer reporting agencies and the Arizona Attorney General, in writing, in a form prescribed by rule or order of the Attorney General or by providing the Attorney General with a copy of the notification provided pursuant to paragraph 1 of this section. A.R.S. § 18-552 (B)(2).
Notification to Regulators	N/A

Notification for Third-Party Data	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. The person that maintains the data under an agreement with the owner or licensee is not required to provide the notifications required by subsection B of this section unless the agreement stipulates otherwise. A.R.S. § 18-552 (C).
Timing of Notification	Within forty-five days after the determination of a breach, the party shall notify the individuals affected. A.R.S. § 18-552 (B).
Private Cause of Action / Enforcement / Penalties	A knowing and willful violation of this section is an unlawful practice pursuant to § 44-1522, and only the Arizona Attorney General may enforce such a violation by investigating and taking appropriate action pursuant to title 44, chapter 10, article 7. The attorney general may impose a civil penalty for a violation of this article not to exceed the lesser of ten thousand dollars per affected individual or the total amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of related breaches may not exceed five hundred thousand dollars. This section does not prevent the attorney general from recovering restitution for affected individuals. A.R.S. § 18-552 (L).
Exceptions	N/A
Other Key Provisions	N/A

State/Territory	**ARKANSAS**
Statute	Ark. Code Ann. § 4-110-101 (West 2019), *et seq.* and Ark. Admin. Code § 214.00.2-5010
Definition of “Personal Information”	“Personal Information” means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted: (A) Social security number; (B) Driver's license number or Arkansas identification card number; (C) 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; (D) Medical information; and (E) (i) Biometric data. (ii) As used in this subdivision (7)(E), “biometric data” means data generated by automatic measurements of an individual's biological characteristics, including without limitation: (a) Fingerprints; (b) Faceprint; (c) A retinal or iris scan; (d) Hand geometry; (e) Voiceprint analysis; (f) Deoxyribonucleic acid (DNA); or (g) Any other unique biological characteristics of an individual if the characteristics are used by the owner or licensee to uniquely authenticate the individual's identity when the individual accesses a system or account. A.C.A. § 4-110-103 (7).
Definition of “Breach”	“Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business. A.C.A. § 4-110-103 (1)(A).
Analysis of Risk of Harm	Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers. A.C.A. § 4-110-105 (d).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	N/A
Unauthorized Employee Disclosure	“Breach of the security of the system” does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure. A.C.A. § 4-110-103 (1)(B).
Notification Obligation	Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A.C.A. § 4-110-105 (a)(1).
Notification to Consumer Reporting Agencies	N/A

Notification to Regulators	Any unauthorized disclosure or breach of a loan applicant's or borrower's financial information or social security number shall be reported by the licensee from whom the information was obtained to the Commissioner within two business days following the date on which the licensee either discovered or, in the exercise of reasonable diligence, should have discovered the unauthorized disclosure or breach.. Ark. Admin. Code § 214.00.07-001 (5005)(1).
Notification for Third-Party Data	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 that there has been a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A.C.A. § 4-110-105 (b)(1). If a breach of the security of a system affects the personal information of more than one thousand (1,000) individuals, the person or business required to make a disclosure of the security breach under subdivision (b)(1) of this section shall, at the same time the security breach is disclosed to an affected individual or within forty-five (45) days after the person or business determines that there is a reasonable likelihood of harm to customers, whichever occurs first, disclose the security breach to the Attorney General. A.C.A. § 4-110-105 (b)(2).
Timing of Notification	The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section, or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. A.C.A. § 4-110-105 (a) (2).
Private Cause of Action / Enforcement / Penalties	Any violation of this chapter is punishable by action of the Attorney General under the provisions of § 4-88-101 *et seq*. A.C.A. § 4-110-108.
Exceptions	The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. A.C.A. § 4-110-105 (c)(1).
Other Key Provisions	N/A

State/Territory	**CALIFORNIA**
Statute	Cal. Civ. Code §§ 1798.80, 1798.82, 1798.84; Cal. Health & Safety Code § 1280.15
Definition of “Personal Information”	“Personal Information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number; (B) driver’s license, 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; (C) account, 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; (D) medical information; (E) health insurance information; (F) unique biometric data generated from measurements or technical analysis of human body characteristics; (G) information or data collected through the use or operation of an automated license plate recognition system; (H) genetic data; or (I) username or email address, in combination with a password or security question and answer that would permit access to an online account. Cal. Civ. Code § 1798.82(h).
Definition of “Breach”	“Breach of the security system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Cal. Civ. Code § 1798.82(g).
Analysis of Risk of Harm	N/A
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Unless an encryption key was or is reasonably believed to have been exposed by the breach, there is no disclosure requirement for a breach of encrypted data. Cal. Civ. Code § 1982.82(a).
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach if the personal information is not used or subject to further unauthorized disclosure. Cal. Civ. Code § 1798.82(g).
Notification Obligation	A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the

	person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. Cal. Civ. Code § 1798.82(a).
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	A person or business that must notify more than 500 California residents as a result of a single breach shall electronically submit a single sample copy of the notification letter to the Attorney General. Cal. Civ. Code § 1798.82(f).
Notification for Third-Party Data	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. Cal. Civ. Code § 1798.82(b).
Timing of Notification	The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Cal. Civ. Code § 1798.82(a).
Private Cause of Action / Enforcement / Penalties	Any customer injured by a violation of this title may bring a civil action to recover damages. Cal. Civ. Code § 1798.84(b).
Exceptions	N/A
Other Key Provisions	N/A

State/Territory	**COLORADO**
Statute	Colo. Rev. Stat. § 6-1-716
Definition of “Personal Information”	‘Personal Information’ means a 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; or biometric data. C.R.S.A. § 6-1-716(1)(g)(I)(A). A 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. C.R.S.A. § 6-1-716(1)(g)(I)(B). A 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. C.R.S.A. § 6-1-716(1)(g)(I)(C).
Definition of “Breach”	‘Security Breach’ means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. C.R.S.A. § 6-1-716(1)(h).
Analysis of Risk of Harm	A covered entity shall give notice to the affected Colorado residents unless the prompt investigation into a security breach determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. C.R.S.A. § 6-1-716(2)(a). A ‘covered entity’ means an individual, business trust, corporation, trust, estate, partnership, unincorporated association or any other legal or commercial entity that maintains, owns, or licenses computerized personal information in the course of their business, vocation, or occupation. C.R.S.A. § 6-1-716(1)(b).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or was reasonably believed to have been acquired. C.R.S. 6-1-716(2)(a.4).
Unauthorized Employee Disclosure	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. C.R.S.A. § 6-1-716(1)(h).
Notification Obligation	In the case of a breach of personal information, notice must include, but need not be limited to: The date (or estimated range) of the breach, a description of what information was acquired through the breach, information that the resident can use to contact the covered entity, the toll-free numbers, addresses, and websites for consumer reporting agencies, the toll-free number, address, and website for the federal trade commission, and a statement that the resident can obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. C.R.S.A. § 6-1-716(2)(a.2)(I)-(VI).
Notification to Consumer Reporting Agencies	If a covered entity is required to notify more than one thousand Colorado residents of a security breach pursuant to this section, the covered entity shall also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal “Fair Credit Reporting Act.” This section does not apply to those covered by the “Gramm-Leach-Bliley Act.” C.R.S.A. § 6-1-716(2)(d).

Notification to Regulators	If a covered entity is required to notify more than one thousand Colorado residents of a security breach pursuant to this section, the covered entity shall also notify, in the most expedient time possible and without unreasonable delay, but not later than 30 days after the determination of a breach, the Colorado Attorney General. C.R.S.A. § 6-1-716(f)(I).
Notification for Third-Party Data	If a covered entity uses a third-party service provider to maintain computerized data that includes personal information, the third-party service provider shall give notice to and cooperate with the covered entity in the event of a breach. Cooperation includes sharing with the covered entity information relevant to the security breach, but need not require the disclosure of confidential business information or trade secrets. C.R.S.A. § 6-1-716(2)(b).
Timing of Notification	Notice must be made in the most expedient time possible and without unreasonable delay, but not more than 30 days after the date of determining that a security breach occurred, but if the covered entity is subject to state or federal laws that maintain procedures for a security breach notification that call for a different notification time period, the shorter time frame controls. C.R.S.A. § 6-7-716(2)(a).
Private Cause of Action / Enforcement / Penalties	The Colorado Attorney General may bring an action in law or equity to address violations of this section to ensure compliance or recover direct economic damages resulting from a violation. Additionally, with either a request from the governor to prosecute or with the approval of the district attorney with jurisdiction to prosecute cases in the judicial district where a case could be brought, the Colorado Attorney General has the authority to prosecute any criminal violations of section 18-5.5-102. C.R.S.A. § 6-7-716(4)-(5).
Exceptions	Pursuant to this section, a covered entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section is in compliance with the notice requirements of this section if the covered entity notifies affected Colorado residents in accordance with its policies in the event of a security breach; except that notice to the attorney general is still required pursuant to subsection (2)(f) of this section. C.R.S.A. § 6-7-716(3)(a). A covered entity that is regulated by state or federal law and that maintains procedures for a security breach pursuant to the laws, rules, regulations, guidances, or guidelines established by its state or federal regulator is in compliance with this section; except that notice to the attorney general is still required pursuant to subsection (2)(f) of this section. C.R.S.A. § 6-7-716(3)(b).
Other Key Provisions	Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the agency has notified the entity not to send the notice as statutorily required. C.R.S.A. § 6-7-716(2)(c).

State/Territory	**CONNECTICUT**
Statute	Conn. Gen. Stat. § 36a-701(b)
Definition of "Personal Information"	An individual's first name or first initial and last name plus any one, or more, of the following data elements: (A) Social Security number; (B) Driver's license number or state identification card number; (C) Credit or debit card number; (D) Financial account number in combination with any required security code, access code or password that would permit access to such financial account. Conn. Gen. Stat. § 36a-701b(a)(2).
Definition of "Breach"	Unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information. The personal information must not be secured by encryption or by any other method or technology that renders the information unreadable or unusable. Conn. Gen. Stat. § 36a-701(b)(a)(1).
Analysis of Risk of Harm	Notification of breach is not required if, after an appropriate investigation and consultation with the relevant federal, state, and local agencies responsible for law enforcement, it is determined that breach will likely not result in harm to the affected Connecticut residents. Conn. Gen. Stat. § 36a-701b(b)(1).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Breach of security only occurs when access to the information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Conn. Gen. Stat. § 36a-701(b)(a)(1).
Unauthorized Employee Disclosure	N/A
Notification Obligation	Any person who conducts business in Connecticut, and who in the ordinary course of the business owns, licenses, or maintains computerized data that includes personal information, must provide notice of any breach of security following the discovery of the breach to any resident of Connecticut whose personal information was breached or is reasonably believed to have been breached. Conn. Gen. Stat. § 36a-701b (b)(1). If notice of a breach of security is required by subdivision (1) of this subsection: (A) The person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General; and (B) The person who conducts business in this state, and who, in the ordinary course of such person's business, owns or licenses computerized data that includes personal information, shall offer to each resident whose personal information under subparagraph (A) of subdivision (4) of subsection (a) of section 38a-999b or subparagraph (A) of subdivision (2) of subsection (a) of this section was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twenty-four months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file. Conn. Gen. Stat. § 36a-701b(b)(2).
Notification to Consumer	N/A

Reporting Agencies	
Notification to Regulators	If notice of a breach of security is required by subdivision (1) of this subsection: […] (B) The person who conducts business in this state, and who, in the ordinary course of such person's business, owns or licenses computerized data that includes personal information, shall offer to each resident whose personal information under subparagraph (A) of subdivision (4) of subsection (a) of section 38a-999b or subparagraph (A) of subdivision (2) of subsection (a) of this section was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twenty-four months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file. Conn. Gen. Stat. § 36a-701b(b)(2)(B).
Notification for Third-Party Data	Any person who maintains computerized data including personal information that the entity does not own, the entity must notify the owner or licensee of the information of any breach of the security of the data immediately upon discovery that personal information of a Connecticut resident was breached or is reasonably believed to have been breached. Conn. Gen. Stat. § 36a-701b(c).
Timing of Notification	Notice must be made without unreasonable delay, but no later than ninety (90) days after the discovery of a breach, unless a shorter time is required by federal law. This notice is subject to the delay of law enforcement or the completion of an investigation to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system. Conn. Gen. Stat. § 36a-701b(b)(1). Notification must be delayed if a law enforcement agency determines that notification will impede a criminal investigation and such law enforcement agency has requested that notification be delayed. After the law enforcement agency determines that notification will no longer compromise the criminal investigation and notifies the person of such determination, notification must be made. Conn. Gen. Stat. § 36a-701b(c).
Private Cause of Action / Enforcement / Penalties	Failure to comply with the requirements of this section constitutes an unfair trade practice for purposes of 42-110b and will be enforced by the Attorney General. Conn. Gen. Stat. § 36a-701b(g).
Exceptions	An information holder that has its own notification procedures as part of an information security policy for the treatment of personally identifiable information shall be considered in compliance with the notification requirements of this section if it notifies the Connecticut resident in accordance with its policies in the event of a breach and if it is otherwise consistent with the timing and notification requirements of this section. Conn. Gen. Stat. § 36a-701b(f). An information holder who has its own security breach procedure pursuant to the rules, regulations, procedures or guidelines established by its primary or functional regulator shall be considered in compliance with the notification requirements of this section if it notifies the Connecticut resident in accordance with its policies in the event of a breach and if it is otherwise consistent with the rules, regulations, procedures or guidelines established by the primary or functional regulator. Conn. Gen. Stat. § 36a-701b(f).
Other Key Provisions	Bulletin IC-25 (August 18, 2010): All licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident that affects Connecticut residents as soon as the incident is identified, but notification must not be any later than five (5) calendar days after the incident is identified.

	Any person in possession of personal information of another person shall safeguard the data, computer files, and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal. Any person who collects Social Security numbers in the course of business shall create a privacy protection policy which shall be published or publicly displayed. Conn. Gen. Stat. § 42a-471(a)-(b).

State/Territory	**DELAWARE**
Statute	6 Del. Code Ann. tit. 6 § 12B-101, *et seq*.
Definition of "Personal Information"	"Personal Information" means a Delaware resident's first name or first initial and last name plus any one or more of the following data elements: (1) Social Security number; (2) driver's license number or state or federal identification card number; (3) account number, credit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account; (4) passport number; (5) a username or email address, in combination with a password or security question and answer that would permit access to an online account; (6) medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health-care professional, or deoxyribonucleic acid profile; (7) health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person; (8) unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes; (9) an individual taxpayer identification number. 6 Del. C. § 12B-101(7).
Definition of "Breach"	"Breach of security" is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. 6 Del. C. § 12B-101(1).
Analysis of Risk of Harm	Disclosure of a breach is required unless after an appropriate investigation, the person reasonably determines that the breach is unlikely to result in harm to the Delaware resident whose personal information has been breached. 6 Del. C. § 12B-102(a).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	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. 6 Del. C. § 12B-101(1)(b).
Unauthorized Employee Disclosure	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. 6 Del. C. § 12B-101(1)(a).
Notification Obligation	Any person who conducts business in Delaware, and who owns or licenses computerized data that includes personal information must provide notice of any breach of security upon determination of the breach of security to any Delaware resident whose personal information was breached or is reasonably believed to have been breached, unless, after an appropriate investigation it is determined that the breach of security is unlikely to result in harm to the resident whose personal information has been breached. 6 Del. C. § 12B-102(a).
Notification to Consumer Reporting Agencies	N/A

Notification to Regulators	If the number of affected Delaware residents to be notified exceeds 500, the person who is required to provide notice must also provide notice of the breach to the Attorney General in a time no later than when notice must be provided to the resident. 6 Del. C. § 12B-102(d).
Notification for Third-Party Data	A person that maintains computerized data that includes personal information that the person does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of security immediately following determination of the breach of security. 6 Del. C. § 12B-102(b).
Timing of Notification	Notification must be made without unreasonable delay, but not later than 60 days after determination of the breach, except in the following situations: (1) a shorter time is required by federal law; (2) a law enforcement agency determines notice will impede a criminal investigation and the law enforcement agency requests that notice be delayed; or (3) when a person could not within 60 days, through reasonable diligence, identify that the personal information of certain Delaware residents were included in a breach of security. Notification must be provided as soon as practicable after the determination that the breach of security includes personal information of Delaware residents. 6 Del. C. § 12B-102(c).
Private Cause of Action / Enforcement / Penalties	The Attorney General may bring an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both. The provisions of Chapter 12 are not exclusive and do not relieve a person subject to this chapter from compliance with all other applicable provisions of law. 6 Del. C. § 12B-104(a).
Exceptions	A person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the person notifies affected Delaware residents in accordance with its policies in the event of a breach of security. 6 Del. C. § 12B-103(a). A person that is regulated by state or federal law, including the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, as amended) and the Gramm Leach Bliley Act (15 U.S.C. § 6801 et. seq., as amended) and maintains its own procedures for a breach of security by following the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the person notifies the affected Delaware residents in accordance with its procedures if a breach occurs. 6 Del. C. § 12B-103(b).
Other Key Provisions	If the breach of security includes a Social Security number, the person shall offer to each resident, whose personal information, including Social Security number, was breached or is reasonably believed to have been breached, credit monitoring services at no cost to such resident for a period of 1 year. 6 Del. C. § 12B-102(e).

State/Territory	**DISTRICT OF COLUMBIA**
Statute	D.C. Code § 28- 3851 *et seq.*
Definition of "Personal Information"	"Personal information" means: (i) an individual's first name, first initial and last name, or any other personal identifier, which, in combination with any of the following data elements, can be used to identify a person or the person's information: (1) Social Security number, Individual Taxpayer Identification Number, passport number, driver's license number, District of Columbia identification card number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (2) account number, credit card number or debit card number, or any other number or code or combination of numbers or codes, such as an identification number, security code, access code, or password, that allows access to or use of an individual's financial or credit account; (3) medical information; (4) genetic information and deoxyribonucleic acid profile; (5) health insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer to identify the person that permits access to an individual's health and billing information; (6) biometric data of an individual generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that is used to uniquely authenticate the individual's identity when the individual accesses a system or account; or (7) any combination of data elements included in sub-sub-subparagraphs (1) through (6) of this sub-subparagraph 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; or (ii) 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 subparagraphs (1) through (6) of sub-subparagraph (i) that permits access to an individual's e-mail account. D.C. Code § 28-3851 (3)(A). "Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. D.C. Code § 28- 3851(3)(B).
Definition of "Breach"	"Breach of the security of the system" means 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 business. D.C. Code § 28-3851(1)(A).
Analysis of Risk of Harm	"Breach of the security system" shall not include: (1) a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized disclosure; (2) acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party unless any information obtained has the potential to compromise the effectiveness of the security protection preventing unauthorized access; or (3) acquisition of personal information of an individual that the person or entity reasonably determines, after a reasonable investigation and consultation with the Office of the Attorney General for the District of Columbia and federal law enforcement agencies, will likely not result in harm to the individual. D.C. Code § 28- 3851(1)(B).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system unless any information obtained has the potential to compromise the effectiveness of the security protection preventing unauthorized access. D.C. Code § 28-3851(1)(B)(ii).
Unauthorized Employee Disclosure	N/A.

Notification Obligation	Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. D.C. Code § 28-3852(a). The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation. D.C. Code § 28-3852(d)
Notification to Consumer Reporting Agencies	If any person or entity is required to notify more than 1,000 persons of a breach of security, the person or entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices. The person or entity is not required to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This requirement does not apply to a person or entity who is required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act. D.C. Code § 28-3852(c).
Notification to Regulators	A person or entity required to give notice shall promptly provide written notice of the breach of the security of the system to the Office of the Attorney General for the District of Columbia if the breach affects 50 or more District residents. This notice shall be made in the most expedient manner possible, without unreasonable delay, and in no event later than when notice is provided under subsection (a) of this section. D.C. Code § 28-3852(b-1).
Notification for Third-Party Data	A person or entity that uses a nonaffiliated third party as a service provider to perform services for a person or entity and discloses personal information about an individual residing in the District under a written agreement with the third party shall require by the agreement that the third party implement and maintain reasonable security procedures and practices. D.C. Code § 28-3852.01(b).
Timing of Notification	The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. D.C. Code § 28-3852(a). The notification required by Section 28-3852 may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation. D.C. Code § 28-3852(d).
Private Cause of Action / Enforcement / Penalties	When a person or entity experiences a breach of the security of the system that requires notification under § 28-3852(a) or (b), and such breach includes or is reasonably believed to include a social security number or taxpayer identification number, the person or entity shall offer to each District resident whose social security number or tax identification number was released identity theft protection services at no cost to such District resident for a period of not less than 18 months. The person or entity that experienced the breach of the security of its system shall provide all information necessary for District residents to enroll in the services required. D.C. Code § 28-3852.02. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law. D.C. Code § 28- 3853(c).
Exceptions	Section 28-3852(c) does not apply to a person or entity who is required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act. D.C. Code § 28-3852(c).

	A person or entity who maintains procedures for a breach notification system under Title V of the Gramm-Leach-Bliley Act, and provides notice as required thereunder to each affected resident in the event of a breach, shall be deemed to be in compliance with the law. D.C. Code § 28- 3852(g).
Other Key Provisions	N/A

State/Territory	**FLORIDA**
Statute	Fla. Stat. § 501.171
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 for that individual: (1) a Social Security number; (2) a driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (3) a financial account number, credit card number, or debit card number with any required security code, access code or password that would permit access to an individual's financial account; (4) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (5) an individual's health insurance policy number, or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or a username or email address, in combination with a password or security question and answer that would permit access to an online account. The term does not include 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. Fla. Stat. § 501.171(1)(g).
Definition of "Breach"	Unauthorized access of data in electronic form containing personal information. Fla. Stat. § 501.171(1)(a).
Analysis of Risk of Harm	Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information. Fla. Stat. § 501.171(2). A covered 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. Fla. Stat. § 501.171(4)(a). Notice to the 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 individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least 5 years. The entity must provide the written determination to the Department within 30 days after the determination. Fla. Stat. § 501.171(4)(c).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The term "Personal Information" does not include 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. Fla. Stat. § 501.171(1)(g).
Unauthorized Employee Disclosure	Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use. Fla. Stat. § 501.171(1)(a).

Notification Obligation	A covered entity shall provide notice to the Department of Legal Affairs of any breach of security affecting 500 or more individuals in Florida. Fla. Stat. § 501.171(3)(a). The written notice to the Department must include: (1) a synopsis of events surrounding the breach at the time notice is provided; (2) the number of individuals in this state who were or potentially have been affected by the breach; (3) any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services; (4) a copy of the notice required under Section 501.171(4) or an explanation of the other actions taken pursuant to Section 501.171(4); the name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach. § 501.171(3)(b). Supplemental information regarding a breach can be provided at any time. Fla. Stat. § 501.171(3)(d). A covered entity shall give notice to each individual in Florida whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Fla. Stat. § 501.171(4)(a). Notice to an affected individual shall be by: (1) written notice sent to the mailing address of the individual in the records of the covered entity; or (2) e-mail notice sent to the e-mail address of the individual in the records of the covered entity. Fla. Stat. § 501.171(4)(d).
Notification to Consumer Reporting Agencies	If an entity discovers circumstances requiring notification pursuant to this section of more than 1,000 individuals at a single time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15. U.S.C. s. 1681(a)(p), of the timing, distribution, and content of the notices. Fla. Stat. § 501.171(5).
Notification to Regulators	For a covered entity that is the judicial branch, the Executive Office of the Governor, the Department of Financial Services, or the Department of Agriculture and Consumer Services, in lieu of providing the written notice to the department, the covered entity may post the information described in Section 501.171(b)(1)-(4) on an agency-managed website. Fla. Stat. § 501.171(3)(e). Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. Fla. Stat. § 501.171(4)(g).
Notification for Third-Party Data	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. Upon receiving notice from a third-party agent, a covered entity shall provide notices required under Sections 501.171(3) and (4). A third-party agent shall provide a covered entity with all information that the covered entity needs to comply with its notice requirements. Fla. Stat. § 501.171(6)(a).
Timing of Notification	A covered entity shall provide notice to the Department of Legal Affairs of a security breach as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred. A covered entity may receive 15 additional days if good cause is provided in writing to the department within 30 days after determination of the breach or reason to believe the breach occurred. Fla. Stat. § 501.171(3)(a). Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify affected individuals, and to restore the reasonable integrity of the breached data system, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay. Fla. Stat. § 501.171(4)(a). If a federal, state, or local law enforcement agency determines that notice to individuals would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period the law enforcement agency deems reasonably necessary. A law enforcement agency may, by written request, revoke or extend the delay. Fla. Stat. § 501.171(4)(b).

Private Cause of Action / Enforcement / Penalties	A violation of Section 501.171 shall be treated as an unfair or deceptive trade practice in any action brought by the department under Section 501.207 against a covered entity or third-party agent. Fla. Stat. § 501.171(9)(a). In addition to the remedies provided for above, a covered entity that violates the notice requirements shall be liable for a civil penalty not to exceed $500,000, as follows: (1) In the amount of $1,000 for each day up to the first 30 days following any violation and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days. (2) If the violation continues for more than 180 days, in an amount not to exceed $500,000. The civil penalties for failure to notify provided apply per breach and not per individual affected by the breach. Fla. Stat. § 501.171(9)(b). All penalties collected shall be deposited into the General Revenue Fund. Fla. Stat. § 501.171(9)(c). Section 501.171 does not establish a private cause of action. Fla. Stat. § 501.171(10).
Exceptions	Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an entity's primary or functional federal regulator is sufficient for compliance in the event of a breach of security. Fla. Stat. § 501.171(4)(g).
Other Key Provisions	All information received by the Department of Legal Affairs pursuant to the notification requirements or pursuant to an investigation by the Department or a law enforcement agency is confidential and exempt from the Public Records requirement under the State Constitution and statutes until such time as the investigation is completed or ceases to be active. Fla. Stat. § 501.171(11).

State/Territory	**GEORGIA**
Statute	O.C.G.A. § 10-1-910 *et seq*
Definition of "Personal Information"	"Personal Information" means an individual's first name or first initial and last name in combination with any one or more of: the following data elements, when either the name or the data elements are not encrypted or redacted: a) social security number; b) driver's license or state ID card number; c) account number, credit card or debit card number, if circumstances exist such that those numbers could be used without additional info, access codes, or passwords; d) Account passwords or personal ID numbers or other access codes; or e) any of the above items standalone (without first name or initial or last name) if the information compromised is sufficient to perform or attempt to perform identity theft against the person whose information was compromised. O.C.G.A. § 10-1-911 (6) "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"	"Breach of the security of the system" means 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. O.C.G.A. § 10-1-911 (1)
Analysis of Risk of Harm	Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach to any resident of GA **whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person**. O.C.G.A. § 10-1-912 (a)
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	In fact-dependent circumstances Statute applies to unencrypted personal information. O.C.G.A. § 10-1-912 (a)
Unauthorized Employee Disclosure	Good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. O.C.G.A. § 10-1-911 (1)
Notification Obligation	Notice may be provided by written or electronically or over the telephone (if the notice provided is consistent with 15 USC § 7001) **Substitute Notice**: If the information broker or data collector demonstrates the cost of notice would exceed $50,000, that the affected class of individuals exceeds 100,000, or that the entity does not have sufficient contact information to provide notice, substitute notice shall consist of all of the following: • Email notice (if information broker or data collector has email addresses for individuals to be notified) • Conspicuous posting of the notice on the information broker's or data collector's website (if the entity maintains one) • Notification to major statewide media

	Notwithstanding any provision of this paragraph to the contrary, an information broker or data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system. O.C.G.A. § 10-1-911 (4)
Notification to Consumer Reporting Agencies	In the event that an information broker or data collector discovers circumstances requiring notification to this Code section of more than 10,000 residents of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 USC § 1681(a), of the timing, distribution, and content of the notices. O.C.G.A. § 10-1-912 (d)
Notification to Regulators	N/A
Notification for Third-Party Data	Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. O.C.G.A. § 10-1-912 (b)
Timing of Notification	Notice shall be made in the **most expedient 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 and restore the reasonable integrity, security, and confidentiality of the data system. O.C.G.A. § 10-1-912 (a)
Private Cause of Action / Enforcement / Penalties	Violation may result in civil penalties.
Exceptions	**Own notification policy:** An information broker or data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.. O.C.G.A. § 10-1-911 (4)(D)(iii)
Other Key Provisions	**Law Enforcement Delay:** The notification required by this Code section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification required by this Code section shall be made after the law enforcement agency determines that it will not compromise the investigation. O.C.G.A. § 10-1-912 (c)

State/Territory	**GUAM**
Statute	9 GCA § 48.10, *et seq.*
Definition of “Personal Information”	“Personal information” means the first name, or first initial, and last name in combination with and linked to any one or more of the following data elements that relate to a resident of Guam, when the data elements are neither encrypted nor redacted: (1) Social Security number; (2) driver’s license number or Guam identification card number issued in lieu of a driver’s license; or (3) 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 a resident’s financial accounts. 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. 9 GCA §§ 48.20(f)
Definition of “Breach”	“Breach of the security of a system” means the 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 Guam. 9 GCA §§ 48.20(a)
Analysis of Risk of Harm	Notification is required if personal information has been accessed or acquired and is reasonably believed will cause, identity theft or other fraud to any resident of Guam. 9 GCA §§ 48.20(a)
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The statute does not apply to personal information that is transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable. 9 GCA §§ 48.20(c) An individual or entity must disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of Guam. 9 GCA §§ 48.30(b)
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided, that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure. 9 GCA §§ 48.20(a)
Notification Obligation	An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification 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. Except as provided in the next paragraph, or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure shall be made without unreasonable delay. 9 GCA §§ 48.30(a)

	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 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. 9 GCA §§ 48.30(c) Notice may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security. 9 GCA §§ 48.30(d) The notification can be made by any of the following methods: • written notice to the postal address in the records of the individual or entity; • telephone notice; • electronic notice; or • substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed Ten Thousand Dollars ($10,000), or that the affected class of residents to be notified exceeds five thousand (5,000) persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice by one of the other three methods. Substitute notice consists of any two (2) of the following: (i) e-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; (ii) conspicuous posting of the notice on the website of the individual or the entity, if the individual or the commercial entity maintains a website; and (iii) notice to major Guam media. 9 GCA §§ 48.20(g)
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	N/A
Notification for Third-Party Data	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 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. 9 GCA §§ 48.30(c).
Timing of Notification	Except as provided in the next paragraph, or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure shall be made without unreasonable delay. 9 GCA §§ 48.30(a) Notice required by this Section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice required by this Section must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security. 9 GCA § 48.30 (d)
Private Cause of Action / Enforcement / Penalties	A violation of this law that results in injury or loss to residents of Guam may be enforced by the Office of the Attorney General. 9 GCA §§ 48.50 (a)

	Except as provided in the "Exceptions" section below, the Office of the Attorney General shall have exclusive authority to bring action and may obtain either actual damages for a violation or a civil penalty not to exceed One Hundred Fifty Thousand Dollars ($150,000) per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. 9 GCA §§ 48.50 (b)
Exceptions	An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this law shall be deemed to be in compliance with the notification requirements of this law if it notifies residents of Guam in accordance with its procedures in the event of a breach of security of the system. 9 GCA §§ 48.40(a) 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 with this law. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional federal regulator shall be in compliance with this law. 9 GCA §§ 48.40(b)
Other Key Provisions	N/A

State/Territory	**HAWAII**
Statute	Haw. Rev. Stat. § 487N-1, *et seq.*
Definition of "Personal Information"	A person'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: (1) Social Security number; (2) driver's license number or Hawaii identification number; (3) account number, credit or debit card, access code, or password that would permit access to an individual's financial account. "Personal Information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. A "record" means any material on which written, drawn, spoken, visual or electromagnetic information is recorded or preserved, regardless of physical form or character. HRS § 487N-1
Definition of "Breach"	An incident of unauthorized access to and acquisition of unencrypted or unreduced 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 the person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. HRS § 487N-1 "Encrypted" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. HRS § 487N-1
Analysis of Risk of Harm	N/A
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The statute does not apply to information that is redacted or encrypted so long as the encryption key was not accessed or is not required. HRS § 487N-1
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of the business 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. HRS § 487N-1
Notification Obligation	Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. HRS § 487N-2 (a) Notice must be clear and conspicuous and must describe: (1) the incident in general terms; (2) the type of personal information that was subject to the breach; (3) the general acts of the business or government agency to protect the personal information from further unauthorized access; (4) a telephone number that the person may call for further

	information and assistance, if one exists; and (5) advice that directs the person to remain vigilant by reviewing account statements and monitoring fee credit reports. HRS § 487N-2 (d) Notice to the affected person may be provided in one of the following methods: (1) written notice to the last available address on record; (2) electronic mail notice if the affected person has agreed to receive communications electronically and if the notice is consistent with the E-SIGN Act [15 U.S.C. section 7001]; or (3) telephonic notice if contact is made directly with the affected person. HRS § 487N-2 (e) Substitute Notice: Substitute notice may be given to certain affected individuals if there is insufficient contact information or consent to satisfy regular notice, if the affected person is unable to be identified, if the cost of providing notice would exceed one hundred thousand dollars ($100,000), or if the affected class of persons exceeds two hundred thousand (200,000). Substitute notice must include all of the following: (1) electronic mail notice when there is an electronic mail address for the affected persons; (2) conspicuous posting of the notice on the website page of the business or agency, of one is maintained, and (3) notification to major statewide media. HRS § 487N-2 (e)(4)
Notification to Consumer Reporting Agencies	Notice to consumers must be made without unreasonable delay consistent with any measures to determine contact information, the scope of the breach and to restore the reasonable integrity, security, and confidentiality of the system. HRS § 487N-2 (a)
Notification to Regulators	In the event a business provides notice to more than one thousand (1000) persons at one time pursuant to this section, the business shall notify in writing, without unreasonable delay, the State of Hawaii's office of consumer protection and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. section 1681a(p), of the timing, distribution, and content of the notice. HRS § 487N-2 (f) A government agency shall submit a written report to the legislature within twenty (20) days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of the security breach, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring. HRS § 487N-4
Notification for Third-Party Data	Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement. HRS § 487N-2 (b)
Timing of Notification	The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system. HRS § 487N-2 (a) Notice may be delayed for any law enforcement agency that informs the business or government agency that notification may impede a criminal investigation or jeopardize national security and requests a delay, so long as the request for delay meets certain requirements. HRS § 487N-2 (c)

Private Cause of Action / Enforcement / Penalties	Any business that violates this statute shall be subject to penalties of not more than two thousand five hundred dollars ($2,500) for each violation. The Hawaii Attorney General of Hawaii or the executive director of the Office of Consumer Protection may bring an action pursuant to this section, however, no such action shall be brought against a government agency. HRS § 487N-3 (a) In addition to any penalty provided for above, any business that violates any provision of this statute shall 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. The court in any action brought under this statute may award reasonable attorneys' fees to the prevailing party. HRS § 487N-3 (b) The penalties provided in this statute shall be cumulative to the remedies or penalties available under all other laws of this State. HRS § 487N-3 (c)
Exceptions	Notification is not required if illegal use of covered information has not occurred nor is reasonably likely to occur, and incident does not create a risk of harm to the person.
Other Key Provisions	Business: This statute applies to any sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. The term also includes an entity whose business is records destruction. HRS § 487N-1 The following businesses shall be deemed to be in compliance with this section: (1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register on March 29, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to the interagency guidance; and (2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996. HRS § 487N-2 (g)

State/Territory	**IDAHO**
Statute	Idaho Stat. § 28-51-104 to 107
Definition of "Personal Information"	Personal Information is an 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: (1) Social Security Number, (2) Driver's License Number or State Identification Card Number, or (3) Account number or credit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media. Idaho Code § 28-51-104 (5)
Definition of "Breach"	Breach means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity. Idaho Code § 28-51-104 (2) This statute covers electronic information only.
Analysis of Risk of Harm	A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident. Idaho Code § 28-51-105 (1)
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	This statute does not apply to information that is encrypted. Idaho Code § 28-51-104 (2)
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of an agency, individual or a commercial entity for the purposes of the agency, individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. Idaho Code § 28-51-104 (2)
Notification Obligation	Notice, if required, must be done by one of the following method: (1) Written Notice (2) Telephonic Notice (3) Electronic Notice (if consistent with 15 U.S.C. § 7001 (E-SIGN))

	Substitute notice, if the agency, individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed twenty-five thousand dollars ($25,000), or that the number of Idaho residents to be notified exceeds fifty thousand (50,000), or that the agency, individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following: (i) E-mail notice if the agency, individual or the commercial entity has e-mail addresses for the affected Idaho residents; and (ii) Conspicuous posting of the notice on the website page of the agency, individual or the commercial entity if the agency, individual or the commercial entity maintains one; and (iii) Notice to major statewide media. Idaho Code § 28-51-104 (4)
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	When an agency becomes aware of a breach of the security of the system, it shall, within twenty-four (24) hours of such discovery, notify the office of the Idaho attorney general. Nothing contained in this section relieves a state agency's responsibility to report a security breach to the office of the chief information officer within the department of administration, pursuant to the Idaho technology authority policies. Idaho Code § 28-51-105 (1)
Notification for Third-Party Data	An agency, individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach. Idaho Code § 28-51-105 (2)
Timing of Notification	Consumer notice, if required, must be made in the most expedient time possible and without unreasonable delay. When an agency becomes aware of a breach of the security of the system, it shall, within twenty-four (24) hours of such discovery, notify the office of the Idaho attorney general. Idaho Code § 28-51-105 (1) Notice required by this section may be delayed if a law enforcement agency advises the agency, individual or commercial entity that the notice will impede a criminal investigation. Notice required by this section must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency advises the agency, individual or commercial entity that notification will no longer impede the investigation. Idaho Code § 28-51-105 (3)
Private Cause of Action / Enforcement / Penalties	An entity that intentionally fails to give notice in accordance with this statute will be subject to a fine of no more than $25,000.00 per breach. Idaho Code § 28-51-107 Any government employee that intentionally discloses personal information not subject to disclosure otherwise allowed by law will be subject to a fine of not more than $2,000.00, or imprisonment in the county jail for a period not more than one year, or both. Idaho Code § 28-51-105 (1) If the primary state regulator believes that an entity has violated the statute (by failing to give notice), the regulator can bring a civil action against the entity to enforce compliance or to enjoin the entity from continued violation. Idaho Code § 28-51-107

Exceptions	An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with section 28-51-105, Idaho Code, if the individual or the commercial entity complies with the maintained procedures when a breach of the security of the system occurs. Idaho Code § 28-51-106 (2) An agency, individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of section 28-51-105, Idaho Code, is deemed to be in compliance with the notice requirements of section 28-51-105, Idaho Code, if the agency, individual or the commercial entity notifies affected Idaho residents in accordance with its policies in the event of a breach of security of the system. Idaho Code § 28-51-106 (1)
Other Key Provisions	N/A

State/Territory	**ILLINOIS**
Statute	815 Ill. Comp. Stat. § 530/1–530/50
Definition of “Personal Information”	Personal Information (PI) is either of the following: (A) a consumer’s first name or first initial and last name plus one or more of the following elements if either the name or the elements neither encrypted nor redacted, or are encrypted or redacted but the keys to unencrypt or unredact were acquired without authorization in the breach: (1) social security number; (2) driver’s license number or state identification card number; (3) account number or credit/debit number in combination with any required security/access code or password that permits access to the consumer’s financial account; (4) medical information; (5) health insurance information; or (6) unique biometric data. (B) a user name or email address in combination with a (1) password or (2) security question and answer permitting access to an online account if either the user name or email address or password or security question and answer are not encrypted nor redacted, or are encrypted or redacted but the keys to unencrypt or unredact were acquired without authorization in the breach. 815 ILCS 530/5
Definition of “Breach”	Breach means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. “Breach of the security of the system data” does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure. 815 ILCS 530/5
Analysis of Risk of Harm	N/A
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	If the PI is encrypted, redacted, and the encryption/redaction key or another means of reading the data was not acquired, then a breach has not occurred.
Unauthorized Employee Disclosure	“Breach of the security of the system data” does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure. 815 ILCS 530/5
Notification Obligation	Any data collector and state agency that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. 815 ILCS 530/10 (a); 815 ILCS 530/12 (a) <u>Breach of PI as defined in subsection (a) above</u>: • <u>Method</u>: Any data collector that owns or licenses nonpublic PI of an Illinois resident must give notification by (1) written notice or (2) electronic notice that is consistent with The E-Sign Act 15 U.S.C. § 7001; and • <u>Content</u>: Including at least: (1) toll free numbers and addresses of consumer reporting agencies; (2) toll-free numbers, addresses, and websites for the FTC; and (3) a statement that the consumer can get information from these sources about fraud alerts and security freezes. <u>Breach of PI as defined in subsection (b) above (emails/usernames)</u>: • <u>Method</u>: Notification in electronic or other form; and

	• Content: Must direct consumers to promptly (1) change their passwords or security question or answer; or (2) take other steps necessary to protect other accounts using this same email address and password or security question and answer. Notice must not include the number of Illinois residents affected by the breach. Substitute Notice: If (1) the cost will exceed $250,000; (2) the number of affected consumers to receive notice exceeds 500,000; or (3) the person lacks sufficient contact information to provide notice, then the person will provide substitute notice through all of the following: (1) emails if the person has them for this class of consumer; (2) conspicuous posting on the person's website (if the person has a website); and (3) notice to major statewide media, or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if the notice is reasonably calculated to give actual notice to the consumers. 815 ILCS 530/10 (c)
Notification to Consumer Reporting Agencies	If a State agency is required to notify more than a thousand (1,000) persons of a breach of security pursuant to this Section, the State agency shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notices. Nothing in this subsection (d) shall be construed to require the State agency to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. 815 ILCS 530/12 (d)
Notification to Regulators	Any data collector required to issue notice pursuant to this Section to more than 500 Illinois residents as a result of a single breach of the security system shall provide notice to the Attorney General of the breach, including: (A) A description of the nature of the breach of security or unauthorized acquisition or use. (B) The number of Illinois residents affected by such incident at the time of notification. (C) Any steps the data collector has taken or plans to take relating to the incident. 815 ILCS 530/10 (e) Any **State agency** that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents shall provide notice to the Attorney General of the breach, including: (A) The types of personal information compromised in the breach. (B) The number of Illinois residents affected by such incident at the time of notification. (C) Any steps the State agency has taken or plans to take relating to notification of the breach to consumers. (D) The date and timeframe of the breach, if known at the time notification is provided. 815 ILCS 530/12 (e)

Notification for Third-Party Data	If data collector maintains PI on behalf of another entity that owns or licenses PI, then person must notify them of breach if PI was or is reasonably believed to have been acquired by an unauthorized person. The data collector must also cooperate with the owner or licensee in matter including, but not limited to, informing the owner or licensee of: (1) the date and nature of the breach; and (2) any steps the data collector has taken or plans to take relating to the breach. 815 ILCS 530/10 (b)
Timing of Notification	Notification must be made in the most expedient time possible and without unreasonable delay but in no event later than when the data collector provides notice to consumers pursuant to this Section. If the date of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date of the breach as soon as possible.. 815 ILCS 530/10 (e) Delayed Notification: The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation. 815 ILCS 530/10 (b-5); 815 ILCS 530/12 (a-5)
Private Cause of Action / Enforcement / Penalties	Private Cause of Action: Those who suffer actual damages may bring a cause under the Consumer Fraud and Deceptive Practices Act. 815 ILCS 530/20
Exceptions	HIPAA Compliance: Those subject to and in compliance with HIPAA will be in compliance with this Act if they must provide notification to the Secretary of Health and Human Services and also provide notification to the Illinois AG within 5 business days of notifying the Secretary. Own Notification Procedures: A data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data. 815 ILCS 530/10 (d)
Other Key Provisions	Any waiver of the provisions of this Act is contrary to public policy and is void and unenforceable. 815 ILCS 530/15 State Agency: • If a state agency that collects PI has a breach of the system data or written material, then the agency must submit a report within 5 business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future security breaches. 815 ILCS 530/25 • If a state agency must notify more than 250 Illinois residents, then the agency must notify the Illinois AG within 45 days or when notifying the consumers (whichever is sooner), unless the State agency has good cause for reasonable delay to determine the scope of the breach and restore the integrity, security, and confidentiality of the data system, or when law enforcement requests in writing to withhold disclosure of some or all of the information required in the notification under this Section. Notification to the AG must include: (1) types of PI compromised; (2) number of Illinoi residents affected; (3) steps the agency has taken or plans to take to notify consumers; (4) the breach's date and time frame in known. 815 ILCS 530/12 (e) • If the State agency that suffers a breach determines the identity of the actor who perpetrated the breach, then the State agency shall report this information, within 5 days after the determination, to the General Assembly. 815 ILCS 530/12 (f) • If the agency is directly responsible to the Governor and has been subject to, or has reason to believe it has been subject to, a single security breach concerning more than 250 Illinois residents' PI, the agency must notify by the Chief Information Security Officer of the Department of Innovation and Technology and the Illinois AG without delay and within 72 hours. 815 ILCS 530/12 (g) • Modified substitute notice provisions apply to state agencies as well.

State/Territory	**INDIANA**
Statute	Ind. Code § 4-1-11 *et seq.*, 24-4.9 *et seq.*
Definition of "Personal Information"	Personal Information means: An individual's first and last name, or first initial and last name, with at least one of the following data elements: (a) Social Security number (b) Driver's License Number or Identification Card Number, (c) Account number, credit card number, debit card number, security code, access code or password of an individual's financial account. Ind. Code Ann. § 4-1-11-3(a) The term does not include the following: (1) The last four (4) digits of an individual's Social Security number. (2) Publicly available information that is lawfully made available to the public from records of a federal agency or local agency. Ind. Code Ann. § 4-1-11-3 (b)
Definition of "Breach"	Breach means unauthorized acquisition at compromises the security, confidentiality or integrity of personal information maintained by a state or local agency. The term does not include the following: (1) Good faith acquisition of personal information by an agency or employee of the agency for purposes of the agency, if the personal information is not used or subject to further unauthorized disclosure. (2) Unauthorized acquisition of a portable electronic device on which personal information is stored if access to the device is protected by a password that has not been disclosed. Ind. Code Ann. § 4-1-11-2 This statute covers electronic and tangible medium if the personal information was transferred from computerized data.
Analysis of Risk of Harm	Consumer notification is not required if the breach has not resulted in and could not result in identity deception, identity theft or fraud.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	This statute does not apply to information that is encrypted or redacted as long as the encryption key was not accessed or acquired. Ind. Code Ann. § 24-4.9-2-5
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an agency or employee of the agency for purposes of the agency, if the personal information is not used or subject to further unauthorized disclosure. Ind. Code Ann. § 4-1-11-3(a)

Notification Obligation	Any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Ind. Code Ann. § 4-1-11-5 (a) Method of Notification: (1) in writing (2) by electronic mail, if the individual has provided the state agency with the individual's electronic mail address. Ind. Code Ann. § 4-1-11-8 This section applies if a state agency demonstrates that: (1) the cost of providing the notice required under this chapter is at least two hundred fifty thousand dollars ($250,000); (2) the number of persons to be notified is at least five hundred thousand (500,000); or (3) the agency does not have sufficient contact information; A state agency may provide the following alternate forms of notice if authorized by subsection (a): (1) Conspicuous posting of the notice on the state agency's web site if the state agency maintains a web site. (2) Notification to major statewide media. Ind. Code Ann. § 4-1-11-9
Notification to Consumer Reporting Agencies	If a state agency is required to provide notice under this chapter to more than one thousand (1,000) individuals, the state agency shall notify without unreasonable delay all consumer reporting agencies (as defined in 15 U.S.C. 1681a) of the distribution and content of the notice. Ind. Code Ann. § 4-1-11-10
Notification to Regulators	If notice is provided to one or more residents of the state, then notice must also be provided to the Attorney General.
Notification for Third-Party Data	A state agency that maintains computerized data that includes personal information, but does not own or license the personal information, must notify the owner or licensee when the entity discovers the personal information was or is reasonably believed to have been accessed by an unauthorized individual. Ind. Code Ann. § 4-1-11-6 (a)
Timing of Notification	Consumer notice, if required, must be given without unreasonable delay. A reasonable delay is one that is: (1) Necessary to restore the integrity of the computer system, (2) Necessary to discover the scope of the breach, or (3) In response to a request from the attorney general or law enforcement agency to delay disclosure Notification may be delayed if law enforcement or the Attorney General requests delay because disclosure will impede a criminal or civil investigation or jeopardize national security. Ind. Code Ann. § 4-1-11-7

Private Cause of Action / Enforcement / Penalties	(a) A person that is required to make a disclosure or notification in accordance with IC 24-4.9-3 and that fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general under this chapter. (b) A failure to make a required disclosure or notification in connection with a related series of breaches of the security of data constitutes one (1) deceptive act. Ind. Code Ann. § 24-4.9-4-1 The attorney general may bring an action under this chapter to obtain any or all of the following: (1) An injunction to enjoin future violations of IC 24-4.9-3. (2) A civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act. (3) The attorney general's reasonable costs in: (a) the investigation of the deceptive act; and (b) maintaining the action. Ind. Code Ann. § 24-4.9-4-2
Exceptions	If an entity maintains its own information privacy policy or security policy that contains a disclosure policy at least as stringent as this statute, the entity is not required to make a separate disclosure under this statute. This section does not apply to an entity that maintains an information privacy policy under: (1) The Gramm-Leach-Bliley Act, (2) The Health Insurance Portability and Accountability Act of 1996 (HIPAA), (3) The USA Patriot Act, (4) Executive Order 13224, (5) The Driver Privacy Protection Act, or (6) The Fair Credit Reporting Act
Other Key Provisions	A person that knowingly or intentionally fails to comply with the database maintenance obligations commits a deceptive act that is actionable only by the state attorney general. Penalties include injunctive relief, a civil penalty of not more than $150,000.00 per violation, and reasonable costs.

State/Territory	**IOWA**
Statute	Iowa Code § 715C.1, 715C.2
Definition of “Personal Information”	A person’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 are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, unredact, or otherwise read the data elements have been obtained through the breach of security: (1) Social Security Number (2) Driver’s License Number or other unique identification number created or collected by a government body, (3) 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, (4) 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, or (5) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data Iowa Code § 715C.1.11
Definition of “Breach”	Breach means unauthorized acquisition of personal information maintained in computerized form by an entity that compromises the security, confidentiality, or integrity of the personal information. Breach of Security also means unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. Iowa Code § 715C.1.1 This statute covers electronic and paper data (if it was printed from a computerized form).
Analysis of Risk of Harm	Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years. Iowa Code § 715C.2.6
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	This statute does not apply when the information is encrypted, redacted, or otherwise altered by any method or technology in such a way that makes it unreadable or unusable without having access to the confidential process or key. Iowa Code § 715C.1.5 To qualify as encrypted, the algorithmic method used must meet accepted industry standards.
Unauthorized Employee Disclosure	Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information. Iowa Code § 715C.1.1

Notification Obligation	Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification, to any consumer whose personal information was included in the information that was breached. Iowa Code § 715C.2.1 Notification must include all of the following: (1) A description of the breach of security (2) The approximate date of the breach of security (3) The type of personal information obtained as a result of the breach of security, (4) Contact information for consumer reporting agencies, and (5) Advice to the consumers to report suspected incidents of identity theft to local law enforcement or the attorney general. Iowa Code § 715C.2.5 Substitute Notice is available if the cost of disclosure exceeds $250,000.00, or if the class of affected individuals exceeds 350,000 individuals, or if the entity does not have sufficient contact information for the affected individuals to provide notice. Iowa Code § 715C.2.4.c
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	If more than 500 Iowa residents are notified, the entity must also notify the Director of the Iowa's Attorney General's Consumer Protection Division within five business days after notifying residents. Iowa Code § 715C.2.8
Notification for Third-Party Data	If the entity maintains personal information on behalf of another entity, the holding entity must notify them immediately following discovery of a breach. Iowa Code § 715C.2.2
Timing of Notification	The entity must provide consumer notice, if required, in the most expeditious manner possible and without unreasonable delay. Iowa Code § 715C.2.1 Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. Notification must be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the entity required to give notice in writing. Iowa Code § 715C.2.3
Private Cause of Action / Enforcement / Penalties	The attorney general may seek and obtain an order that a party, held to violate this section, pay damages to the attorney general on behalf of a person injured by the data breach violation. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law. Iowa Code § 715C.2.9
Exceptions	This statute does not apply to an entity that complies with notification requirements or breach of security procedures that provide greater protection of personal information and disclosure requirements that are at least as comprehensive as this statute. Iowa Code § 715C.2.7.a

	This statute does not apply to an entity that is in compliance with a state or federal law that provides greater protection and disclosure requirements than this statute. Iowa Code § 715C.2.7.b This statute does not apply to an entity that is subject to, and complies with, regulations under Title V of the Gramm-Leach-Bliley Act. Iowa Code § 715C.2.7.c This statute does not apply to an Entity that is subject to and complies with the regulations promulgated pursuant to Title II, subtitle F of the Health Insurance Portability and Accountability Act (HIPAA) and Title XIII, subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH). Iowa Code § 715C.2.7.d
Other Key Provisions	N/A

State/Territory	**KANSAS**
Statute	Kan. Stat. Ann. §50-7a01–50-7a04.
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 if the data elements are neither encrypted nor redacted: (1) social security number; (2) driver’s license number or state identification card number; or (3) financial account number or credit card number alone or in combination with any required security/access code or password that permits access to the consumer’s financial account. K.S.A. § 50-7a01 (g)
Definition of “Breach”	Breach means unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality, or integrity of PI maintained by an individual or a commercial entity (person) and that causes, or such person reasonably believes has caused or will cause, identity theft to any consumer. K.S.A. § 50-7a01 (h)
Analysis of Risk of Harm	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 shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident. K.S.A. § 50-7a02 (a)
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	If the information is encrypted, redacted, unreadable, or unusable, then this is not PI and a breach has not occurred.
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure. K.S.A. § 50-7a01 (h)
Notification Obligation	Any person that conducts business in Kansas, or a government, or governmental subdivision or agency that owns or licenses computerized data that includes PI must give notification by (1) written notice or (2) electronic notice that is consistent with The E-Sign Act 15 U.S.C. § 7001. (This appears restricted to those business operating in Kansas.) (3) Substitute Notice: If (a) the cost will exceed $100,000; (b) the number of affected consumers to receive notice exceeds 5,000; or (3) the person lacks sufficient contact information to provide notice. K.S.A. § 50-7a01 (c)
Notification to Consumer Reporting Agencies	If a breach in this section requires notifying more than 1,000 people at one time, then the person must also notify without unreasonable delay all nationwide consumer reporting agencies that compile and maintain files on consumers, as defined by 15 U.S.C. § 1681a(p), of the timing distribution, and content of the notices. .) K.S.A. § 50-7a02 (f)
Notification to Regulators	NA

Notification for Third-Party Data	If person maintains PI on behalf of another entity, then person must notify them of breach if PI was or is reasonably believed to have been accessed or acquired by an unauthorized person. (This appears broader than the provision addressing owners or licensees because this provision applies to those outside of Kansas.) K.S.A. § 50-7a02 (b)
Timing of Notification	Notice must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the computerized data system's reasonable integrity. K.S.A. § 50-7a02 (a) Delayed Notification: Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this section shall be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.. K.S.A. § 50-7a02 (c)
Private Cause of Action / Enforcement / Penalties	Non-Insurance Providers: For violations of this section, except as to insurance companies licensed to do business in this state, the attorney general is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law. K.S.A. § 50-7a02 (g) Insurance Providers: Kansas Insurance Commissioner has the sole authority to enforce this section. K.S.A. § 50-7a02 (h)
Exceptions	Own Notification Procedures: Notwithstanding any other provision in this section, an individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the individual or the commercial entity notifies affected consumers in accordance with its policies in the event of a breach of security of the system.. K.S.A. § 50-7a02 (d) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section. . K.S.A. § 50-7a02 (e)
Other Key Provisions	

State/Territory	**KENTUCKY**
Statute	Ky. Rev. Stat. § 365.732
Definition of “Personal Information”	Personal information means an individual’s first name or first initial and last name plus any one or more of the following data elements, when the name or data element is not redacted: (1) Social Security number; (2) Driver’s license number; or (3) 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. KRS § 365.732 (1)(c)
Definition of “Breach”	Breach means 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 the Commonwealth of Kentucky. KRS § 365.732 (1)(a)
Analysis of Risk of Harm	N/A
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The statute is triggered by the unauthorized acquisition of unencrypted and unredacted computerized data. Therefore, the statute does not apply to information that is encrypted or redacted. KRS § 365.732 (1)(a)
Unauthorized Employee Disclosure	Good-faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure. KRS § 365.732 (1)(a)
Notification Obligation	Upon discovery or notification of a breach, any Kentucky resident whose unencrypted information was or is reasonably believed to have been acquired by an unauthorized person must be notified. Disclosure must be consistent with the needs of law enforcement or any measures that are necessary to determine the scope of the breach and restore the reasonable integrity of the data system. KRS § 365.732 (2)
Notification to Consumer Reporting Agencies	If a person discovers that notification is required to more than one thousand (1,000) persons at one time, the person must also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files of the timing, distribution, and content of the notices. KRS § 365.732 (7)
Notification to Regulators	N/A
Notification for Third-Party Data	If you conduct business in Kentucky, and you hold computerized data that includes personally identifiable information that you do not own, as the holder you must notify the owner or licensee of the information of any breach as soon as reasonably practicable following discovery, if the personally identifiable information was, or is reasonably believed to have been acquired by an unauthorized person. KRS § 365.732 (3)

Timing of Notification	The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (4) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. KRS § 365.732 (2) A delay of notification is proper if a law enforcement agency determines that notification will impede a criminal investigation. After the law enforcement agency determines that notification will not compromise the investigation, notification must be made promptly. KRS § 365.732 (4)
Private Cause of Action / Enforcement / Penalties	N/A
Exceptions	An information holder that has its own notification procedures as part of an information security policy for the treatment of personally identifiable information shall be considered in compliance with the notification requirements of this section if it notifies the subject persons in accordance with its policies in the event of a breach and if it is otherwise consistent with the timing requirements of this section. KRS § 365.732 (6)
Other Key Provisions	The provisions of this section do not apply to any person who is subject to the provisions of Title V of the Gramm-Leach Bliley Act of 1999, as amended, or the federal Health Insurance Portability and Accountability Act of 1996, as amended, or any agency of the Commonwealth of Kentucky or any of its local governments or political subdivisions. KRS § 365.732 (8)

State/Territory	**LOUISIANA**
Statute	La. Rev. Stat. § 51:3071-77 La. Admin. Code Tit. 16, § 701
Definition of "Personal Information"	A person's first name or first initial and last name plus one or more of the following: (1) Social Security Number, (2) Driver's License Number or State Identification Card Number, (3) An account, credit or debit card number in combination with the required security code, access code or password that would permit access to the individual's financial account, (4) Passport Number, or (5) Biometric Data La. R.S. § 51:3073 (4)
Definition of "Breach"	Breach means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to personal information maintained by an agency or person. La. R.S. § 51:3073(2) This statute covers electronic information only.
Analysis of Risk of Harm	Notification will not be required if, after reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to the residents of Louisiana. The person or business must retain a copy of the written determination (including supporting documentation) for five years from the date of discovery of the breach of the security system. If requested in writing, the person or business must send a copy of the written determination (including supporting documentation) to the attorney general no later than 30 days from the date of receipt of the written request. La. R.S. § 51:3074 (I)
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	This statute does not apply to information that is encrypted or redacted.
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person is not a breach of the security of the system, provided that the personal information is not used for, or is subject to, unauthorized disclosure. La. R.S. § 51:3073(2)

Notification Obligation	Notification may be provided by one of the following methods: (1) Written notification. (2) Electronic notification, if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001. (3) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed one hundred thousand dollars, or that the affected class of persons to be notified exceeds one hundred thousand, or the agency or person does not have sufficient contact information. Substitute notification shall consist of all of the following: (a) E-mail notification when the agency or person has an e-mail address for the subject persons. (b) Conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained. Notification to major statewide media La. R.S. § 51:3074 (G)
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	If notice to Louisiana residents is required, the person or entity must also provide written notice to the Consumer Protection Section of the Attorney General's office. Notice must be received with 10 days of distribution of notice to Louisiana residents. The notice must include the names of the affected residents. La. R.S. § 51:3074 (I)
Notification for Third-Party Data	After discovery of a breach, any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that maintains computerized data, that includes personal information that the agency or person does not own, must 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. La. R.S. § 51:3074 (D)
Timing of Notification	Notification must be made in the most expedient time possible and without unreasonable delay, but not later than 60 days from discovery of the breach. La. R.S. § 51:3074 (E) If notification is delayed by law enforcement request or due to a determination by the entity that measures are necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system, the entity shall provide the attorney general the reasons for the delay in wring within the 60-day notification period. Upon receipt of the notification, the attorney general will permit a reasonable extension. La. R.S. § 51:3074 (F)

Private Cause of Action / Enforcement / Penalties	An individual may file a civil action to recover actual damages resulting from the failure to disclose, in a timely manner, to a person that there has been a breach that resulted in the disclosure of the individual's personal information. La. R.S. § 51:3075 Failure to provide timely notice to the attorney general may be punishable by a fine no to exceed $5,000.00 per violation. Each day that notice is not received is a new, separate violation. A violation of the notification requirement is an unfair act or trade practice under R.S. 51:1405(A). La. R.S. § 51:3074 (J)
Exceptions	An agency or person that maintains a notification procedure as part of its information security policy for the treatment of personal information which is otherwise consistent with the timing requirements of this Section shall be considered to be in compliance with the notification requirements of this Section if the agency or person notifies subject persons in accordance with the policy and procedure in the event of a breach of security of the system. La. R.S. § 51:3074 (H)
Other Key Provisions	A financial institution that is subject to and compliant with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice will be deemed to be in compliance with this statute. La. R.S. § 51:3076

State/Territory	**MAINE**
Statute	10 Me. Rev. Stat. § 1346 *et seq.*
Definition of “Personal Information”	Personal information is 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: (1) social security number; (2) driver's license number or state identification card number; (3) 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; (4) account passwords or personal identification numbers or other access codes. Or Any of the data elements in the above paragraphs (1) - (4) when not in connection with the individual's first name, or first initial, and last name, if the information compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the individual whose information was compromised. “Personal information” does not include information from 3rd-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. 10 M.R.S. § 1347.6
Definition of “Breach”	Breach means an unauthorized acquisition, release or use of an individual's computerized data that includes PI that compromises the security, confidentiality or integrity of PI of the individual maintained by an entity. 10 M.R.S. § 1347.1
Analysis of Risk of Harm	If any entity (individual or information broker) who maintains computerized data including PI becomes aware of a breach, that entity shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that PI has been or will be misused. If the entity determines that misuse of PI has occurred or is reasonably possible that misuse will occur, they shall give notice of a breach. 10 M.R.S. § 1348.1
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Does not apply to information that is encrypted or redacted, so long as the encryption key was not accessed or acquired.
Unauthorized Employee Disclosure	Good faith acquisition, release or use of PI by an employee or agent of a person on behalf of the entity is not a breach if the PI is not used for or subject to further unauthorized disclosure to another person. 10 M.R.S. § 1347.1

Notification Obligation	If an entity that maintains computerized data including PI becomes aware of a breach, the entity shall give notice of the breach following discovery or notification of the breach to a resident of ME whose PI has been acquired by an unauthorized person. 10 M.R.S. § 1348.1 Notice can be provided by written or electronic notice if consistent with E-SIGN. Substitute notice available if certain criteria are satisfied.
Notification to Consumer Reporting Agencies	If more than 1,000 individuals must be notified at a single time, the entity must notify all consumer reporting agencies without unreasonable delay. Notification must include the date of the breach, an estimate of the number of individuals affected by the breach, if known, and the actual or anticipated date that individuals were or will be notified of the breach. 10 M.R.S. § 1348.4
Notification to Regulators	When notice is required, the entity shall notify the Department of Professional and Financial Regulation state regulators, or if the entity is not regulated by the Department, the state Attorney General. 10 M.R.S. § 1348.5
Notification for Third-Party Data	A third-party that maintains, on behalf of another entity, computerized data including PI that the third-party does not own shall notify the owner of the PI of a breach immediately following discovery if PI was, or is reasonably believed to have been, acquired by an unauthorized person. 10 M.R.S. § 1348.2
Timing of Notification	Notices must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data in the system. If there is no delay of notification due to law enforcement investigation, the notices must be made no more than 30 days after the person becomes aware of a breach of security and identifies its scope. 10 M.R.S. § 1348.1 Delay for Law Enforcement: If, after the completion of an investigation to determine the likelihood that PI has been or will be misused notification is required, the notification may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation. 10 M.R.S. § 1348.3
Private Cause of Action / Enforcement / Penalties	Private Cause of Action: The rights and remedies available under this section are cumulative and do not affect or prevent rights and remedies available under federal or state law. 10 M.R.S. § 1349.3 Attorney General Enforcement: Enforced by state Attorney General and/or where applicable, the Department of Professional and Financial Regulation Office of Consumer Credit Regulation. 10 M.R.S. § 1349.1 An entity who violates this chapter commits a civil violation and is subject to one or more of the following: (1) A fine of not more than $500 per violation, up to a maximum of $2,500 for each day the entity is in violation of this chapter, except that this paragraph does not apply to State Government, the University of Maine System, the Maine Community College System or Maine Maritime Academy; (2) equitable relief; or (3) enjoinment from further violations of this chapter. 10 M.R.S. § 1349.2
Exceptions	A person that complies with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to federal law or the law of this State is deemed to be in compliance with the requirements of section 1348 as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements of section 1348. 10 M.R.S. § 1349.4

Other Key Provisions	N/A

State/Territory	**MARYLAND**
Statute	Md. Code Com. Law § 14-3501 *et seq*.
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 the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: (1) Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government; (2) A driver's license number or State identification card number; (3) 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; (4) Health information, including information about an individual's mental health; (5) 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; or (6) Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, 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. Or A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account. Md. COMMERCIAL LAW Code Ann. § 14-3501(e)(1)
Definition of "Breach"	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the PI maintained by a business. Md. COMMERCIAL LAW Code Ann. § 14-3504(a)(1)
Analysis of Risk of Harm	When the entity discovers or is notified that it incurred a breach of the security of a system, it shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach. Md. COMMERCIAL LAW Code Ann. § 14-3504(b)(1)
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Does not apply to information that is encrypted, redacted or otherwise protected by another method that renders the info unreadable or unusable. Md. COMMERCIAL LAW Code Ann. § 14-3501(e)(1)(i)
Unauthorized Employee Disclosure	"Breach" does not include the good faith acquisition of PI by an employee or agent of a business for the purposes of the business, provided that the PI is not used or subject to further unauthorized disclosure. Md. COMMERCIAL LAW Code Ann. § 14-3504(a)(2)
Notification Obligation	Notice must include: a description of categories of info (including elements of PI) acquired; covered entity's address, telephone number, and toll-free number; toll-free numbers and addresses of the major CRAs; and toll-free numbers, addresses, and websites for the FTC and MD Attorney General, plus a statement that residents can obtain info from these sources about steps to avoid identity theft. Md. COMMERCIAL LAW Code Ann. § 14-3504(g)

	Notice can be provided in writing, by email (if resident expressly consented to receive electronic notices or if business is primarily conducted online), or by telephone. Substitute notice is available if certain criteria are satisfied. Electronic notice permitted in the case of a breach involving PI that permits access to an email account only, but specific content and delivery requirements apply. Md. COMMERCIAL LAW Code Ann. § 14-3504(e)
Notification to Consumer Reporting Agencies	If an entity must notify 1,000 or more individuals, the entity also shall notify, without unreasonable delay, each CRA that compiles and maintains files on consumers on a nationwide basis of the timing, distribution, and content of the notices. Md. COMMERCIAL LAW Code Ann. § 14-3506
Notification to Regulators	Prior to giving the required notification for individuals, an entity shall provide notice of a breach of the security of a system to the state Office of the Attorney General. Md. COMMERCIAL LAW Code Ann. § 14-3504(h)
Notification for Third-Party Data	A third-party that maintains computerized data including PI of an individual residing in MD that the entity does not own or license shall notify the owner or licensor of the PI of a breach if it is likely that the breach has resulted or will result in the misuse of PI of an individual residing in MD. Notification required by a third-party shall be given as soon as practicable but not later than 45 days after the entity discovers or is notified of the breach. Md. COMMERCIAL LAW Code Ann. § 14-3504(c)
Timing of Notification	Notices must be given as soon as reasonably practicable, but no later than 45 days after the business concludes the investigation, consistent with measures necessary to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system. Md. COMMERCIAL LAW Code Ann. § 14-3504(b)(3) Delay for Law Enforcement: Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or jeopardize homeland or national security. Notification shall be given as soon as reasonably practicable but not later than 30 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security. Md. COMMERCIAL LAW Code Ann. § 14-3504(d)
Private Cause of Action / Enforcement / Penalties	Private Cause of Action: Consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act. Attorney General Enforcement. Violations are subject to the enforcement and penalty provisions contained in the unfair or deceptive trade practice provisions, including: injunction, damages, attorney's fees, and civil penalties not to exceed $1,000 per violation for first-time offenders and $5,000 per violation for repeat offenders. Md. COMMERCIAL LAW Code Ann. § 14-3508
Exceptions	Primary Regulator: An entity that complies with the requirements for notification procedures under the rules, regulations, procedures, or guidelines established by the primary or functional federal or state regulator of the entity shall be deemed to be in compliance with the statute. Md. COMMERCIAL LAW Code Ann. § 14-3504(k); Md. COMMERCIAL LAW Code Ann. § 14-3507(b) Gramm-Leach-Bliley Act: An entity or the affiliate that is subject to and in compliance with the Gramm-Leach-Bliley Act, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions, shall be deemed to be in compliance. Md. COMMERCIAL LAW Code Ann. § 14-3507(c) HIPAA: An entity or affiliate of the Entity that is in compliance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed to be in compliance. Md. COMMERCIAL LAW Code Ann. § 14-3507(d)
Other Key Provisions	N/A

State/Territory	**MASSACHUSETTS**
Statute	Mass. Gen. Laws 93H § 1, *et seq.*
Definition of "Personal Information"	A resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (1) Social Security number; (2) driver's license number or state-issued identification card number; or (3) 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 However, that PI shall 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. M.G.L.A. 93H, § 1 (a)
Definition of "Breach"	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 PI, maintained by an entity that creates a substantial risk of identity theft or fraud against a resident of MA. M.G.L.A. 93H, § 1 (a) *Data is defined as any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics. M.G.L.A. 93H, § 1 (a)
Analysis of Risk of Harm	If the definition of "breach" is not met, then notice is not required.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Does not apply to information that is encrypted, so long as encryption key was not compromised.
Unauthorized Employee Disclosure	Good faith but unauthorized acquisition of PI by an entity, or employee or agent thereof, for the lawful purposes of such entity, is not a breach unless the PI is used in an unauthorized manner or subject to further unauthorized disclosure. M.G.L.A. 93H, § 1 (a)
Notification Obligation	Notice must include information about resident's right to obtain a police report, how to 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, and mitigation to be provided. Notification must not include the nature of the incident or the number of residents affected by the incident. M.G.L.A. 93H, § 3(b) Notice can be provided in writing or electronic notice (if consistent with E-SIGN and Mass. Gen Laws ch 110G). Substitute notice is available if certain criteria are satisfied. *See* M.G.L.A. 93H, § 1 (a)
Notification to Consumer Reporting Agencies	The entity shall provide notice to CRAs, and the notice shall include the nature of the breach of security or unauthorized acquisition or use, the number of residents in MA affected by the breach at the time of notification, the name and address of the person or agency that experienced the breach of security, the name and title of the person or agency reporting the breach, and their relationship to the person or agency that experience the breach, the type of person or agency reporting the breach, the

	person responsible for the breach (if known), the type of PI compromised, whether the entity maintains a written information security program, and any steps the person or agency has taken or plans to take relating to the incident. M.G.L.A. 93H, § 3 (b)
Notification to Regulators	An entity must notify the state Attorney General and Director of OCABR as soon as practicable and without unreasonable delay. The notice must include the nature of the breach of security or unauthorized acquisition or use, the number of residents in MA affected by the breach at the time of notification, the name and address of the person or agency that experienced the breach of security, the name and title of the person or agency reporting the breach, and their relationship to the person or agency that experience the breach, the type of person or agency reporting the breach, the person responsible for the breach (if known), the type of PI compromised, whether the entity maintains a written information security program, and any steps the person or agency has taken or plans to take relating to the incident. M.G.L.A. 93H, § 3 (b) If an agency is within the Executive Department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use of the information to the Executive Office of Technology Services and the Division of Public Records as soon as practicable and without unreasonable delay following discovery of the breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident. M.G.L.A. 93H, § 3 (e)
Notification for Third-Party Data	A third-party that maintains information including PI on behalf of another entity must notify them as soon as practicable and without unreasonable delay when the third-party knows or has reason to know of a breach or unauthorized acquisition or use of PI. The third-party must cooperate with the owner or licensor of the covered info, including specific disclosure obligations. M.G.L.A. 93H, § 3 (a)
Timing of Notification	As practicable and as not to impede active investigation by the attorney general or other law enforcement agency, the office of consumer affairs and business regulation shall: (i) make available electronic copies of the sample notice sent to consumers on its website and post such notice within 1 business day upon receipt from the person that experienced a breach of security; (ii) update the breach of security notification report on its website as soon as practically possible after the information has been verified by said office but not more than 10 business days after receipt unless the information provided is not verifiable. M.G.L.A. 93H, § 3 (c) Delay for Law Enforcement: Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and has notified the Attorney General, in writing. Notice required must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. M.G.L.A. 93H, § 4
Private Cause of Action / Enforcement / Penalties	Attorney General Enforcement: The attorney general may bring an action against an entity or otherwise to remedy violations of this chapter and for other relief that may be appropriate. Penalties include civil penalties, damages, and injunctive relief. M.G.L.A. 93H, § 6 A person that experienced a breach of security shall not require a resident to waive the resident's right to a private right of action as a condition of the offer of credit monitoring services. M.G.L.A. 93H, § 3A (b)
Exceptions	Primary Regulator: Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an entity's primary or functional state or federal regulator is sufficient for compliance. M.G.L.A. 93H, § 5
Other Key Provisions	N/A

State/Territory	**MICHIGAN**
Statute	Mich. Comp. Laws §§ 445.63, .72
Definition of "Personal Information"	The first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state: (1) Social security number; (2) Driver license number or state personal identification card number; or (3) 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. MCLA § 445.63 (r)
Definition of "Breach"	Unauthorized access and acquisition of data that compromises the security or confidentiality of PI maintained by an entity as part of a database of PI regarding multiple residents. MCLA § 445.63 (b)
Analysis of Risk of Harm	Notification not required if entity determines that breach has not and is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one of more MI residents. MCLA § 445.72 (1) This section does not apply to the access or acquisition by a person or agency of federal, state, or local government records or documents lawfully made available to the general public. MCLA § 445.72 (17)
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Does not apply to information that is encrypted or redacted so long as encryption key was not accessed or acquired. MCLA § 445.72 (1)(a)-(b)
Unauthorized Employee Disclosure	"Breach" does not include unauthorized access to data by an employee or other person if the access meets all of the following: (1) The employee or other person acted in good faith in accessing the data; (2) The access was related to the activities of the entity; and (3) The employee or other person did not misuse any PI or disclose any PI to an unauthorized person. MCLA § 445.63 (b)
Notification Obligation	Notice must be communicated in a clear and conspicuous manner; describe the breach in general terms; describe the type of covered info subject to the breach; generally describe steps taken to protect data against further breaches, if applicable; provide a telephone number the resident may call for assistance or additional info; and remind the resident of the need to remain vigilant for incidents of fraud and identity theft. MCLS § 445.72 (6) Notice can be provided by written, electronic or telephone notice. The statute specifies requirements for each type of notice. Substitute notice is available if certain criteria are satisfied. MCLA § 445.72 (5)
Notification to Consumer	If an entity notifies 1,000 or more MI residents, and is not subject to 15 USC 6801 to 6809, the entity shall, after notifying those residents, notify each CRA that compiles and maintains files on consumers on a nationwide basis of the security breach without unreasonable delay. MCLA § 445.72 (8) This subsection does not apply if the entity is subject to Title V of the Gramm-Leach-Bliley Act.

Reporting Agencies	
Notification to Regulators	N/A
Notification for Third-Party Data	Any third-party that maintains a database that includes data that the third-party does not own or license that discovers a breach shall provide a notice to the owner or licensor of the information of the security breach, unless the third-party determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to one or more residents of MI. MCLA § 445.72 (2)
Timing of Notification	An entity shall provide notice without unreasonable delay, consistent with measures necessary to determine the scope and breach and restore reasonable integrity of the database. MCLA § 445.72 (4) Delay for Law Enforcement: Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or jeopardize homeland or national security. Notification shall be given as soon as reasonably practicable after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security. MCLA § 445.72 (4)(b)
Private Cause of Action / Enforcement / Penalties	This does not affect the availability of any civil remedy for a violation of state or federal law. Attorney general enforcement MCLA § 445.67a (3) Entities who fail to provide notice may be ordered to pay a civil fine of not more than $250 for each failure to provide notice, capped at $750,000 per security breach. MCLA § 445.72 (13), (14) Criminal penalties for notice of a security breach that has not occurred, where such notice is given with the intent to defraud. The offense is a misdemeanor, punishable by imprisonment for not more than 93 days or a fine of not more than $250 per violation (or both). (Second and third violations have same penalty, except that the fine increases to $500 and $750, respectively.) MCLA § 445.72 (12) Similarly, entities who distribute an advertisement or make any other solicitation that misrepresents to the recipient that a security breach has occurred that may affect the recipient are punishable by imprisonment for not more than 93 days or a fine of not more than $1,000 per violation (or both). (Second and third violations have same penalty, except that the fine increases to $2,000 and $3,000, respectively. MCLA § 445.72b. (3) The aggregate liability of a person for civil fines under subsection (13) for multiple violations of subsection (13) that arise from the same security breach shall not exceed $750,000.00. MCLA § 445.72 (14)
Exceptions	Federal Interagency Guidance: A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision shall be deemed to be in compliance. MCLA § 445.72 (9) HIPAA-Covered Entities: A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter. MCLA § 445.72 (10)

	Insurers: Entities subject to, or regulated under MI's insurance code are exempt from the state’s data breach notification statute and instead will be governed by HB 6491/Public Act 690 of 2018, which goes into effect January 20, 2021. An entity that is subject to or regulated under the insurance code of 1965, 1965 PA 218, MCL 500.100 to 500.8302, is exempt from this act. MCLA § 445.64 (1)
Other Key Provisions	Provides that entities may deliver notice pursuant to an agreement with another entity, if the agreement does not conflict with MI law.

State/Territory	**MINNESOTA**
Statute	Minn. Stat. § 325E.61
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: (1) Social Security number; (2) driver's license number or Minnesota identification card number; or (3) 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. Minn. Stat. § 325E.61. Subd. 1. (e)
Definition of “Breach”	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the entity. Minn. Stat. § 325E.61. Subd. 1. (d)
Analysis of Risk of Harm	N/A
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Does not apply to information that is encrypted or secured by another method of technology that renders it unreadable or unusable, so long as the encryption key, password, or other means necessary for reading or using the data is not also acquired. Minn. Stat. § 325E.61. Subd. 1. (e)
Unauthorized Employee Disclosure	Good faith acquisition of PI by an employee or agent of the entity for the purposes of the entity is not a breach, provided that the PI is not used or subject to further unauthorized disclosure. Minn. Stat. § 325E.61. Subd. 1. (d)
Notification Obligation	Any entity to which the statute applies shall disclose any breach following discovery or notification of the breach in the security of the data to any resident of MN whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person. Minn. Stat. § 325E.61. Subd. 1. (a) Notice can be provided by written notice to most recent address in covered entity’s records, or electronic notice if the primary method of communication with the resident or if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied. Minn. Stat. § 325E.61. Subd. 1. (g)
Notification to Consumer Reporting Agencies	If an entity notifies more than 500 individuals at one time, the entity shall also notify, within 48 hours, all CRAs that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices. § 325E.61. Subd. 2

Notification to Regulators	N/A
Notification for Third-Party Data	Any third-party that maintains data that includes PI that the third-party does not own shall notify the owner or licensor of the information of any breach immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person. Minn. Stat. § 325E.61. Subd. 1. (b)
Timing of Notification	The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system. Minn. Stat. § 325E.61. Subd. 1. (a) Delay for Law Enforcement: Notice may be delayed to a date certain if a law enforcement agency affirmatively determines that the notice will impede a criminal investigation. Minn. Stat. § 325E.61. Subd. 1. (c)
Private Cause of Action / Enforcement / Penalties	There is no private right of action for violations of the Minnesota's data-breach notice statute. *In re Target Corp. Data Sec. Breach Litigation*, 66 F. Supp. 3d 1154, 1168 (D. Minn. 2014). Attorney general enforcement. Minn. Stat. § 325E.61. Subd. 6
Exceptions	Own Notification Policy: An entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and whose procedures are otherwise consistent with the timing requirements of the statute, shall be deemed to be in compliance with the notification requirements, if the entity notifies subject individuals in accordance with its policies in the event of a breach. Minn. Stat. § 325E.61. Subd. 1. (h) Exemption for "financial institution" as defined by 15 U.S.C. § 6809(3). Minn. Stat. § 325E.61. Subd. 4
Other Key Provisions	N/A

State/Territory	**MISSISSIPPI**
Statute	Miss. Code § 75-24-29
Definition of “Personal Information”	An individual’s first name or first initial and last name plus one or more of the following: (1) Social Security Number, (2) Driver’s License Number or State Identification Card Number, or (3) An account number or credit or debit card number in combination with the required security code, access code or password that would permit access to the individual’s account (4) “Affected individual” means any individual who is a resident of MS whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security. Miss. Code Ann. § 75-24-29 (2)(b)
Definition of “Breach”	The unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information of any resident of Mississippi 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. Miss. Code Ann. § 75-24-29 (2)(a)
Analysis of Risk of Harm	Notification is not required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals. Miss. Code Ann. § 75-24-29 (3)
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Notice is not required if the data is encrypted or made unusable or unreadable by another method or technology. Miss. Code Ann. § 75-24-29 (2)(a)
Unauthorized Employee Disclosure	N/A
Notification Obligation	A person who conducts business in Mississippi shall disclose any breach of security to all affected individuals. Miss. Code Ann. § 75-24-29 (3) Notification shall be provided by one of the following methods: (1) Written Notice, (2) Telephone Notice, (3) Electronic Notice (if the person’s primary means of communication with the affected individual is by electronic means, or if the notice is consistent with 15 U.S.C.S. § 7001 (E-SIGN)), or Substitute notice is available (if the cost of providing Written, Telephone or Electronic Notice exceeds $5,000.00, or if the class of affected individuals exceeds 5,000 individuals, or if the person does not have sufficient contact information) Miss. Code Ann. § 75-24-29 (6)

Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	N/A
Notification for Third-Party Data	Any person who conducts business in Mississippi that maintains computerized data which includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of the security of the data 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. Miss. Code Ann. § 75-24-29 (4)
Timing of Notification	Disclosure must be made without unreasonable delay. Miss. Code Ann. § 75-24-29 (3) Notification shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed. Notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and notifies the person of that determination. Miss. Code Ann. § 75-24-29 (5)
Private Cause of Action / Enforcement / Penalties	Failure to comply with this statute constitutes unfair trade practices and shall be enforced by the Attorney General. This statutes does not create a private cause of action. Miss. Code Ann. § 75-24-29 (8)
Exceptions	Notification will not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individual. Miss. Code Ann. § 75-24-29 (3) Any person who conducts business in Mississippi and the business maintains its own security breach procedures as part of an information security policy and complies with the timing requirements of this statute shall be deemed to be in compliance with the notification requirements of this section if the person notifies the affected individuals in accordance with the business' policies. Miss. Code Ann. § 75-24-29 (7)
Other Key Provisions	N/A

State/Territory	**MISSOURI**
Statute	Mo. Rev. Stat. § 407.1500
Definition of "Personal Information"	Personal Information is a state 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 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: (1) Social Security number (2) Driver's license number or other unique identification number created or collected by a government body (3) 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 (4) 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 (5) Medical information (6) Health insurance information § 407.1500. 1 (9) R.S.Mo.
Definition of "Breach"	Unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person who compromises the security, confidentiality, or integrity of the personal information. § 407.1500. 1 (1) R.S.Mo. This statute covers electronic information only.
Analysis of Risk of Harm	Notification is not required if after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. . § 407.1500. 2 (5) R.S.Mo. This determination must be documented in writing and the documentation must be kept for five years.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	This statute does not apply to information that is encrypted, redacted or otherwise altered in such a manner to make it unreadable or unusable. § 407.1500. 1 (9) R.S.Mo.
Unauthorized Employee Disclosure	Good faith acquisition of PI by a person or that person's employee or agent for a legitimate purpose of that person is not a breach, provided that the PI is not used in violation of applicable law or in a manner that harms or poses an actual threat of security, confidentiality, or integrity of the PI. § 407.1500. 1 (1) R.S.Mo.
Notification Obligation	Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach. § 407.1500. 2 (1) R.S.Mo.

	Consumer notice, if required, must include: (1) A general description of the breach (2) The type of covered information affected (3) A telephone number for further information and assistance, if one exists (4) Contact information from Consumer Reporting Agencies (5) Advice to remain vigilant by reviewing account statements and monitoring free credit reports § 407.1500. 2 (4) R.S.Mo. Notice must be made by one of the following methods: (1) In Writing (2) By Telephone (if contact is made directly with affected resident) (3) Electronic Notice (if entity has a valid email address, the individual agrees to receive communications electronically, and notice is consistent with E-SIGN) Substitute notice is available if the cost of providing notice would exceed $100,000.00, or the class of affected consumers is greater than 150,000, or the entity does not have sufficient contact information or consent, or the entity is unable to identify particular affected consumers. § 407.1500. 2 (6) R.S.Mo.
Notification to Consumer Reporting Agencies	If more than 1,000 state residents are notified, the entity must, without unreasonable delay, notify all nationwide Consumer Reporting Agencies of the timing, distribution, and content of the consumer notice. § 407.1500. 2 (8) R.S.Mo.
Notification to Regulators	If more than 1,000 state residents are notified, the entity must, without unreasonable delay, notify the attorney general's office of the timing, distribution, and content of the notice. § 407.1500. 2 (8) R.S.Mo.
Notification for Third-Party Data	If an entity maintains covered information on behalf of another, the entity must notify the owner immediately following the discovery of a breach. § 407.1500. 2 (2) R.S.Mo.
Timing of Notification	Notice, if required, must be made without unreasonable delay. § 407.1500. 2 (1) R.S.Mo. Notification may be delayed if law enforcement informs the entity that notification will impede a criminal investigation or jeopardize national or homeland security. The request by law enforcement to delay notification must be in writing or otherwise documented by the covered entity contemporaneously. The documentation must also include the law enforcement officer's name and agency. § 407.1500. 2 (3) R.S.Mo.
Private Cause of Action / Enforcement / Penalties	The Attorney General has exclusive authority to bring an action for actual damages from a willful and knowing violation of this statute. The Attorney General may seek a civil penalty of no more than $150,000.00 per breach of the security system or series of breaches of a similar nature that are discovered in a single investigation. § 407.1500. 4 R.S.Mo.
Exceptions	Any entity that maintains its own security breach procedures as part of an information security policy and complies with the timing requirements of this statute will be deemed to be in compliance with the notification requirements of this section if the person notifies the affected individuals in accordance with the business' policies. § 407.1500. 3 (1) R.S.Mo.

	A person that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the person notifies affected consumers in accordance with the maintained procedures when a breach occurs. § 407.1500. 3 (2) R.S.Mo. Financial Institutions compliant with the following will be deemed in compliance with this statute: (1) Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, or (2) The National Credit Union Administration regulations in 12 CFR Part 748, or (3) The Gramm-Leach-Bliley Act § 407.1500. 3 (3) R.S.Mo.
Other Key Provisions	N/A

State/Territory	**MONTANA**
Statute	Mont. Code Ann. §§ 30-14-1701, *et seq*.
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: (1) Social security number; (2) Driver's license number, state identification card number, or tribal identification card number; (3) An 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 person's financial account; (4) Medical record information as defined in 33-19-104; (5) Taxpayer identification number; or (6) An identity protection personal identification number issued by the IRS. § 30-14-1704(4)(b).
Definition of "Breach"	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. § 30-14-1704(4)(a).
Analysis of Risk of Harm	Any entity to which the statute applies shall disclose any breach of the security of the data system following discovery or notification of the breach to any Montana resident whose **unencrypted personal information** was or **is reasonably believed to have been acquired by an unauthorized person.** § 30-14-1704(1).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The statute applies only to disclosures of unencrypted information. § 30-14-1701(1).
Unauthorized Employee Disclosure	Good faith acquisition of PI by an employee or agent of the person or business for the purposes of the person or business is not a breach, provided the PI is not used or subject to further unauthorized disclosure. § 30-14-1704(4)(a).
Notification Obligation	Notice may be provided by: • Written notice • Electronic notice (consistent with 15 U.S.C. § 7001 E-SIGN) • Telephonic notice, or • Substitute notice, if (a) notice cost exceeds $250,000, (b) affected class of subject persons to be notified exceeds 500,000, or (c) the entity does not have sufficient contact information. Substitute notice must consist of: ○ Electronic mail notice when the entity has an electronic mail address for the subject persons; and ○ Conspicuous posting of the notice on the entity's web page, if one is maintained; or ○ Notification to applicable local or statewide media. § 30-14-1704(5).

Notification to Consumer Reporting Agencies	If a business notifies an individual of a breach and suggests, indicates, or implies that the individual may obtain a credit report, the business must coordinate with the credit reporting agency as to the timing, content, and distribution of notice to the individual (but this may not unreasonably delay disclosure of the breach). § 30-14-1704(7).
Notification to Regulators	Any person or business that is required to issue a notification 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. § 30-14-1704(8).
Notification for Third-Party Data	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 system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person. § 30-14-1704(2).
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. § 30-14-1704(1). The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation. § 30-14-1704(3).
Private Cause of Action / Enforcement / Penalties	**Department Action:** Whenever the department has reason to believe that a person has violated this part and that proceeding would be in the public interest, the department may bring an action in the name of the state against the person to restrain by temporary or permanent injunction or temporary restraining order the use of the unlawful method, act, or practice upon giving appropriate notice to that person. § 30-14-1705(1).
Exceptions	**Own Notification Policy.** A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered to be in compliance with the notification requirements of the statute if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the data system. § 30-14-1704(6).
Other Key Provisions	**N/A**

State/Territory	**NEBRASKA**
Statute	Neb. Rev. Stat. §§ 87-801, *et seq*.
Definition of “Personal Information”	Personal information includes the following 1. The combination of a Nebraska resident’s first name or first initial and last name along with any of the following data elements that are not encrypted, redacted, or otherwise altered by technology such that the name or data elements are unreadable: (1) Social Security number; (2) motor vehicle operator’s license number or state identification card number; (3) 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; (4) unique electronic identification number or routing code, in combination with any required security code, access code, or password; or (5) unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation. § 87-802(5)(a). 2. The combination of a username or email address and a password or security question and answer that would permit access to an online account. § 87-802(5)(b).
Definition of “Breach”	The unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity, excluding certain good-faith acquisitions by employees or agents. § 87-802(1).
Analysis of Risk of Harm	Notification is required if a reasonable and prompt investigation determines that unauthorized information about a Nebraska resident has occurred or is likely to occur. § 87-803(1).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	As long as the encryption key was not accessed or acquired. § 87-802(5).
Unauthorized Employee Disclosure	Good faith acquisition of PI by an employee or agent of an individual or commercial entity for the purposes of the individual or commercial entity is not a breach of security if the PI is not used or subject to further unauthorized disclosure. § 87-802(1).
Notification Obligation	Once an individual or commercial entity, to which the statute applies, becomes aware of a breach and determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, it must give notice to the Nebraska resident. If the individual or commercial entity determines that it is unlikely that personal information has been or will be used for an unauthorized purpose, notification is not required. § 87-803(1).
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	If notice of a security breach to a Nebraska resident is required, notice of the breach must be provided to the Attorney General at the same time. § 87-803(2).
Notification for Third-Party Data	The owner or licensee of the information of any breach of the security of the data system must be notified immediately following discovery of a breach. § 87-803(3).

Timing of Notification	Notice shall be made as soon as possible and without unreasonable delay, 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. § 87-803(1). Delay for Law Enforcement: Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. § 87-803(4).
Private Cause of Action / Enforcement / Penalties	The Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of section 87-803. § 87-806(1). A violation does not give rise to a private cause of action. § 87-806(2).
Exceptions	Own Notification Policy: An entity that maintains its own notice procedures which are part of an information security policy for the treatment of personal information and which are otherwise consistent with the timing requirements of the statute, is deemed to be in compliance with the notice requirements of the statute if the entity notifies affected NE residents and Attorney General in accordance with its notice procedures in the event of a breach of the security of the system. § 87-804(1). Compliance with Other Laws: An individual or commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with the notice requirements of the statute if the individual or commercial entity notifies affected Nebraska residents and the Attorney General in accordance with the maintained procedures in the event of a breach of the security of the system. § 87-804(2).
Other Key Provisions	1. Waiver Not Permitted. § 87-805. 2. Acquisition of PI pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach. § 87-802(1).

State/Territory	**NEVADA**
Statute	Nev. Rev. Stat. §§ 603A.010, *et seq.*
Definition of “Personal Information”	A natural person’s first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (a) Social Security number; (b) Driver’s license number, driver authorization card number or identification card number; (c) Account number, credit card or debit card number, in combination with any required security code, access code or password that would permit access to the person’s financial account; (d) A medical identification number or a health insurance identification number; (e) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account. § 603A.040.
Definition of “Breach”	The unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the data collector who handles, collects, disseminates, or deals with nonpublic personal information. §§ 603A.020-030.
Analysis of Risk of Harm	Notification is required upon breach.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	This statute does not apply to encrypted personal information. § 603A.220(1).
Unauthorized Employee Disclosure	Breach does not include the good faith acquisition of PI by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the PI is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure. § 603A.020.
Notification Obligation	Any data collector that owns or licenses computerized data which includes personal information must disclose a breach of the security system 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. § 603A.220(1). Notice may be provided by one of the following methods: (a) Written notification; (b) Electronic notification (if consistent with E-SIGN); (c) Substitute notification if (1) the cost of providing notification would exceed $250,000, (2) the affected class exceeds 500,000, or (3) the data collector does not have sufficient contact information. § 603A.220(4).
Notification to Consumer Reporting Agencies	If more than 1,000 Nevada residents are to be notified at one time, the data collector must notify (without unreasonable delay) any Consumer Reporting Agency that compiles and maintains files on consumers on a nationwide basis, of the time notification is distributed and the content of the notification. § 603A.220(6).
Notification to Regulators	N/A

Notification for Third-Party Data	Any data collector who maintains computerized data that includes personal information, that the data collector does not own, the data collector must inform the owner or licensee of the information of any breach of security immediately following discovery that personal information was, or is reasonably believed to have been, acquired by an unauthorized individual. § 603A.220(2).
Timing of Notification	If a breach to any resident of Nevada occurs, disclosure must be made in the most expedient time possible and without unreasonable delay. This notice is subject to the needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. § 603A.220(1). A delay of notification is proper if a law enforcement agency determines that notification will impede a criminal investigation. After the law enforcement agency determines that the notification will no longer compromise the investigation, notification required by this section must be made. § 603A.220(3).
Private Cause of Action / Enforcement / Penalties	Rights of Data Collector: A data collector who provides the proper notification based on this statute may commence an action for damages against a person who unlawfully acquired or benefitted from personal information from the data collector's records. § 603A.270. The Attorney General or a district attorney who has reason to believe that a person is violating, proposes to violate, or has violated the provisions of this statute may bring an action against that person to obtain a temporary or permanent injunction against that violation. § 603A.290. The Attorney General may also institute an appropriate legal proceeding against an operator if the Attorney General has reason to believe that an operator, either directly or indirectly, has violated or is violating section 603A.340 or section 603A.345. The district court may issue a temporary or permanent injunction or impose a civil penalty not to exceed $5,000 for each violation. § 603A.360(2). No private right of action. § 603A.360(3).
Exceptions	If a data collector has its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section, it will be deemed in compliance with the notification requirements of this section if the data collector notifies the proper people in accordance with its policies and procedures. § 603A.220(5)(a). If a data collector is subject to the data privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.*, the data collector will be deemed in compliance with the notification requirements of this section. § 603A.220(5)(b).
Other Key Provisions	Waiver is not permitted. § 603A.100.

State/Territory	**NEW HAMPSHIRE**
Statute	N.H. Rev. Stat. §§ 359-C:16, C:19-21.
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, when either the name or the data elements are not encrypted: 1) Social Security number; 2) Driver's license number or other government identification number; or 3) 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. § 359-C:19(IV)(a). Personal information shall not include information that is lawfully made available to the general public from federal, state, or local government records. § 359-C:19(IV)(b).
Definition of "Breach"	An unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. § 359-C:19(V).
Analysis of Risk of Harm	Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision. § 359-C:20(I)(a).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	This statute does not apply to information that is encrypted or secured by a method that renders it completely unreadable or unusable so long as the encryption key was not also acquired. § 359-C:19(II), (IV)(a).
Unauthorized Employee Disclosure	Good faith acquisition of PI by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the PI is not used or subject to further unauthorized disclosure. § 359-C:19(V).
Notification Obligation	The notice required under this section shall be provided by one of the following methods: a) Written notice. b) Electronic notice, if the agency or business' primary means of communication with affected individuals is by electronic means. c) Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons. d) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the person does not have sufficient contact information or consent to provide notice pursuant to subparagraphs I(a)-I(c). Substitute notice shall consist of all of the following: (1) E-mail notice when the person has an e-mail address for the affected individuals; (2) Conspicuous posting of the notice on the person's business website, if the person maintains one; (3) Notification to major statewide media. e) Notice pursuant to the person's internal notification procedures maintained as part of an information security policy for the treatment of personal information. § 359-C:20(III).

	Notice under this section shall include at a minimum: a) A description of the incident in general terms. b) The approximate date of breach. c) The type of personal information obtained as a result of the security breach. d) The telephonic contact information of the person subject to this section. § 359-C:20(IV).
Notification to Consumer Reporting Agencies	If a person is required to notify more than 1,000 consumers of a breach of security pursuant to this section, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice. § 359-C:20(VI)(a).
Notification to Regulators	Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the NH attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in NH who will be notified. Nothing in this section shall be construed to require the person to provide to any regulator or the New Hampshire attorney general's office the names of the individuals entitled to receive the notice or any personal information relating to them. The disclosure shall be made to affected individuals as quickly as possible, after the determination required under this section. § 359-C:20(I)(b).
Notification for Third-Party Data	Any person or business that maintains computerized data that includes personal information that the person or business does not own shall 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. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets. § 359-C:20(I)(c).
Timing of Notification	The person shall notify the affected individuals as soon as possible as required under this subdivision. § 359-C:20(I)(a). Notification may be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security. § 359-C:20(II).
Private Cause of Action / Enforcement / Penalties	Any person injured by any violation under this subdivision may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. If the court finds for the plaintiff, recovery shall be in the amount of actual damages. If the court finds that the act or practice was a willful or knowing violation of this chapter, it shall award as much as 3 times, but not less than 2 times, such amount. In addition, a prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Any attempted waiver of the right to the damages set forth in this paragraph shall be void and unenforceable. Injunctive relief shall be available to private individuals under this chapter without bond, subject to the discretion of the court. § 359-C:21(I). The New Hampshire attorney general's office shall enforce the provisions of this subdivision pursuant to RSA 358-A:4. § 359-C:21(II). The burden shall be on the person responsible for the determination under RSA 359-C:20, I to demonstrate compliance with this subdivision. § 359-C:21(III).
Exceptions	Any person engaged in trade or commerce that is subject to RSA 358-A:3, I which maintains procedures for security breach notification pursuant to the laws, rules, regulations, guidances, or guidelines issued by a state or federal regulator shall be deemed to be in compliance with this subdivision if it acts in accordance with such laws, rules, regulations, guidances, or guidelines. § 359-C:20(V).

Other Key Provisions	Waiver not permitted. § 359-C:21(I); § 359-C:16.

State/Territory	**NEW JERSEY**
Statute	N.J. Stat. Ann. §§ 56:8-161, 163, 165 – 166.
Definition of "Personal Information"	An individual's first name or first initial and last name linked with any one or more of the following data elements: 1) Social Security number; 2) driver's license number or State identification card number; 3) 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; or 4) (4) 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. Personal information shall 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. § 56:8-161.
Definition of "Breach"	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. § 56:8-161.
Analysis of Risk of Harm	Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach 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. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years. § 56:8-163(a).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	This statute does not apply to information that is encrypted or secured by any other method or technology that renders it unreadable or unusable. § 56:8-161.
Unauthorized Employee Disclosure	Good faith acquisition of PI by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the PI is not used for a purpose unrelated to the business or subject to further unauthorized disclosure. § 56:8-161.
Notification Obligation	Notice may be provided by one of the following methods: 1) Written notice; 2) Electronic notice, if the notice provided is consistent with 15 U.S.C. § 7001 (E-SIGN); or 3) Substitute notice, if the business or public entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business or public entity does not have sufficient contact information. Substitute notice shall consist of all of the

	following: (a) E-mail notice when the business or public entity has an e-mail address; (b) Conspicuous posting of the notice on the Internet web site page of the business or public entity, if the business or public entity maintains one; and (c) Notification to major Statewide media. § 56:8-163(d).
Notification to Consumer Reporting Agencies	In addition to any other disclosure or notification required under this section, in the event that a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s. 1681a), of the timing, distribution and content of the notices. § 56:8-163(f).
Notification to Regulators	Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities. § 56:8-163(c)(1).
Notification for Third-Party Data	Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, 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. § 56:8-163(b).
Timing of Notification	The disclosure to a customer shall 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 restore the reasonable integrity of the data system. § 56:8-163(a). The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity. § 56:8-163(c)(2).
Private Cause of Action / Enforcement / Penalties	Any willful, knowing, or reckless violation of the data breach notification requirement is an unlawful practice and a violation of Title 56, Chapter 8 of the New Jersey Statutes. § 56:8-166. In addition to appropriate legal or equitable relief, a court may award a person who suffers an ascertainable financial or property loss as a result of a violation of the Act threefold their actual damages, plus fees and costs. § 56:8-19. The attorney general has enforcement authority and may seek remedies including injunctive relief (§ 56:8-8), civil penalties of not more than $10,000 for the first offense and not more than $20,000 for each later offense (§ 56:8-13), and costs (§ 56:8-11).
Exceptions	A business or public entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and is otherwise consistent with the requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the business or public entity notifies subject customers in accordance with its policies in the event of a breach of security of the system. § 56:8-163(e).
Other Key Provisions	N/A

State/Territory	**NEW MEXICO**
Statute	N.M. Stat. Ann. §§ 57-12C-1 to 57-12C-12.
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 when they are not encrypted, redacted, or otherwise rendered unreadable or unusable: (1) social security number; (2) driver's license number or government-issued identification number; (3) account number or credit/debit card number in combination with any required security or access code or password that permits access to the person's financial account; or (4) biometric data. Information lawfully obtained from publicly available sources or from federal, state, or local government records lawfully made available to the general public is not personal information. § 57-12C-2(C).
Definition of "Breach"	Unauthorized acquisition of unencrypted computerized data, or of unencrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality, or integrity of personal information maintained by a person. § 57-12C-2(D).
Analysis of Risk of Harm	Notification is not required if an appropriate investigation determines that the breach does not give rise to a significant risk of identity theft or fraud. § 57-12C-6(B).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	If the data element is encrypted, redacted, unreadable, or unusable, then this is not personal information and a breach has not occurred provided the confidential process or key to decrypt the encrypted data was not accessed or acquired. § 57-12C-2(C), (D).
Unauthorized Employee Disclosure	A good faith acquisition of personal identifying information by an employee or agent of an entity for a legitimate business purpose of the entity is not a security breach, provided that the personal information is not subject to further unauthorized disclosure. § 57-12C-2(D).
Notification Obligation	Method: A person that owns or licenses computerized data that includes personal information of a New Mexico resident must give notification by (1) U.S. mail; (2) electronic notice if this is the normal method of communication with the New Mexico resident or provided that electronic notice is consistent with 15 U.S.C. § 7001; or (3) substitute notice if the person demonstrates that (a) the cost will exceed $100,000; (b) the number of affected New Mexico residents to receive notice exceeds 50,000; or (c) the person lacks sufficient contact information to provide notice. § 57-12C-6(A), (D). Contents: (1) Name and contact information of the notifying person; (2) a list of the types of personal information reasonably believed to have been breached (if known); (3) the estimated date or range of dates within which the breach occurred (if known); (4) a general description of the security breach incident; (5) the toll-free numbers and addresses of the major consumer reporting agencies; (6) consumer advice to check credit reports and accounts for errors resulting from the breach; and (7) advice that informs the consumer of her rights under the federal Fair Credit Reporting Act. § 57-12C-7.
Notification to Consumer Reporting Agencies	If a breach in this section requires notifying more than 1,000 New Mexico residents at one time, then the person must also notify a nationwide consumer reporting agency in the most expedient time possible and no later than 45 days after the discovery of the breach. § 57-12C-10.
Notification to Regulators	If a breach in this section requires notifying more than 1,000 people at one time, then the person must also notify the New Mexico Attorney General in the most expedient time possible, and no later than 45 days after the breach's discovery. The entity must include the number of residents that received notification and a copy of that notification. § 57-12C-10.
Notification for Third-Party Data	If a person maintains personal information on behalf of an owner or licensee, the person must notify the owner or licensee of a breach., if an appropriate investigation determines that the breach does not give rise to a significant risk of identity theft or fraud. § 57-12C-6(C).

Timing of Notification	Most expedient time possible, and not later than 45 calendar days following discovery of a breach and consistent with any measures necessary to determine the scope of the breach and restore the computerized data system's reasonable integrity, security, and confidentiality. § 57-12C-6.
Private Cause of Action / Enforcement / Penalties	There is no private right of action. However, the Attorney General may bring actions for violations of this statute on behalf of individuals. In such action, a court may issue (1) injunctions; (2) damages of actual costs or losses; and (3) civil penalties of the greater of a $25,000 penalty or $10 per failed notification up to $150,000. § 57-12C-11.
Exceptions	Delayed Notification: When requested by law enforcement or as necessary to determine the scope of the breach and restore reasonable integrity of the computerized data system. § 57-12C-9. Own Notification Procedures: If a person's own notification procedures, as part of an information security policy for personal information treatment, are consistent with New Mexico's notification timing requirements, then the person does not violate this section if the person notifies consumers in accordance with its policies in the event of a breach. § 57-12C-6(F). HIPAA: This statute does not apply to a person subject to HIPAA. § 57-12C-8. Financial Institutions: This statute does not apply to a person subject to the Gramm-Leach-Bliley Act. § 57-12C-8.
Other Key Provisions	N/A.

State/Territory	**NEW YORK**
Statute	N.Y. Gen. Bus. Law § 899-AA.
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. § 899-AA(1)(a). “Private information” shall mean either (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired: (1) Social security number; (2) Driver's license number or non-driver identification card number; (3) Account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (4) 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; or (5) Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or (ii) A user name or e-mail address in combination with a password or security question and answer that would permit access to an online account. “Private information” does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records. *Note: Private information is the only information that triggers a breach notification in New York. § 899-AA(2).
Definition of “Breach”	Unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business. § 899-AA(1)(c). In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person. § 899-AA(1)(c).
Analysis of Risk of Harm	In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

	1) Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; 2) Indications that the information has been downloaded or copied; or 3) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported. § 899-AA(1)(c).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	When private information is encrypted and the encryption key has not been accessed or acquired, there is no duty to notify. § 899-AA(1)(b).
Unauthorized Employee Disclosure	Good faith access to, or acquisition of, private information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure. § 899-AA(1)(c)
Notification Obligation	Any person or business which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. § 899-AA(2). The notice required by this section shall be directly provided to the affected persons by one of the following methods: (1) Written notice; (2) Electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction; (3) Telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or (4) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. § 899-AA(5). Substitute notice shall consist of all of the following: (a) E-mail notice when such business has an e-mail address for the subject persons, except if the breached information includes an e-mail address in combination with a password or security question and answer that would permit access to the online account, in which case the person or business shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online account; (b) Conspicuous posting of the notice on such business's web site page, if such business maintains one; and (c) Notification to major statewide media. § 899-AA(5).

	Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired. § 899-AA(7).
Notification to Consumer Reporting Agencies	In the event that more than 5,000 New York residents are to be notified at one time, the person or business shall also notify "consumer reporting agencies" as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents. § 899-AA(8)(b). "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section. § 899-aa(1)(d).
Notification to Regulators	In the event that more than 5,000 New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents. § 899-AA(8)(a). Any covered entity required to provide notification of a breach, including breach of information that is not "private information," to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary. § 899-AA(9).
Notification for Third-Party Data	Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. § 899-AA(3).
Timing of Notification	The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the integrity of the system. § 899-AA(2).
Private Cause of Action / Enforcement / Penalties	Whenever the attorney general shall believe from evidence satisfactory to him or her that there is a violation of this article he or she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to twenty dollars per instance of failed notification, provided that the latter amount shall not exceed two hundred fifty thousand dollars. § 899-AA(6)(a). The remedies provided by this section shall be in addition to any other lawful remedy available. § 899-AA(6)(b).

	No action may be brought under the provisions of this section unless such action is commenced within three years after either the date on which the attorney general became aware of the violation, or the date of notice sent to affected New York residents, whichever occurs first. In no event shall an action be brought after six years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach. § 899-AA(6)(c).
Exceptions	Notice to affected persons 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 persons 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 years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination. § 899-AA(2)(a). If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the division of state police and to consumer reporting agencies: (1) Regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time; (2) Regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time; (3) Part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the State of New York, as amended from time to time; or (4) Any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.§ 899-AA(2)(b).
Other Key Provisions	This statute preempts any provisions of local law, ordinance, or code. § 899-AA(10).

State/Territory	**NORTH CAROLINA**
Statute	N.C. Gen. Stat. §§ 75-61, 75-65.
Definition of “Personal Information”	A person's first name or first initial and last name in combination with any of the following identifying information (as defined in G.S. 14-113.20(b)): 1) Social security or employer taxpayer identification numbers. 2) Driver’s license, State identification card, or passport numbers. 3) Checking account numbers. 4) Savings account numbers. 5) Credit card numbers. 6) Debit card numbers. 7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6). 8) Digital signatures. 9) Any other numbers or information that can be used to access a person's financial resources. 10) Biometric data. 11) Fingerprints. § 75-61(10). Additionally, if, and only if, any of the following information “would permit access to a person’s financial account or resources,” it is considered personal information when taken in conjunction with a person’s first name, or first initial and last name: 1) Electronic identification numbers 2) Electronic mail names or addresses 3) Internet account numbers 4) Internet identification names. 5) Passwords. 6) Parent's legal surname prior to marriage. § 75-65(a). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records. § 75-61(10).
Definition of “Breach”	An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of 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. § 75-61(14).
Analysis of Risk of Harm	Notification is required if the personal information accessed or acquired is unencrypted and unredacted, or contains 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 § 75-61(14).
Safe Harbor for Data that is Encrypted,	Any incident of 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. § 75-61(14).

Unreadable, Unusable, or Redacted?	
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of the business 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. § 75-61(14).
Notification Obligation	Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. § 75-65(a). The notice shall be clear and conspicuous. The notice shall include <u>all</u> of the following: 1) A description of the incident in general terms. 2) A description of the type of personal information that was subject to the unauthorized access and acquisition. 3) A description of the general acts of the business to protect the personal information from further unauthorized access. 4) A telephone number for the business that the person may call for further information and assistance, if one exists. 5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. 6) The toll-free numbers and addresses for the major consumer reporting agencies. 7) The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft. § 75-65(d). For purposes of this section, notice to affected persons may be provided by <u>one</u> of the following methods: 1) Written notice. 2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001. 3) Telephonic notice provided that contact is made directly with the affected persons. 4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following: a. E-mail notice when the business has an electronic mail address for the subject persons. b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained. c. Notification to major statewide media. § 75-65(e).
Notification to Consumer Reporting Agencies	In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, 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 in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. § 75-65(f).
Notification to Regulators	In the event a business provides notice to an affected person pursuant to this section, the business shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of 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. § 75-65(e1).

Notification for Third-Party Data	Any business that maintains or possesses records or data containing personal information of residents of North Carolina 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 shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement. § 75-65(b).
Timing of Notification	The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. § 75-65(a). The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security. § 75-65(c).
Private Cause of Action / Enforcement / Penalties	A violation of this section is a violation of G.S. 75-1.1 (civil and criminal penalties are available). § 75-65(i). No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation. Causes of action arising under this Article may not be assigned. § 75-65(i), (j).
Exceptions	A financial institution that is subject to and 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, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or a credit union that 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; and any revisions, additions, or substitutions relating to any of the said interagency guidance, shall be deemed to be in compliance with this section. § 75-65(h).
Other Key Provisions	Any waiver of the provisions of this Article is contrary to public policy and is void and unenforceable. § 75-65(g).

State/Territory	**NORTH DAKOTA**
Statute	N.D. Cent. Code §§ 51-30-01, *et seq*.
Definition of “Personal Information”	An individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: 1) The individual's social security number; 2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14; 3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1; 4) The individual's financial institution 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 accounts; 5) The individual's date of birth; 6) The maiden name of the individual's mother; 7) Medical information; 8) Health insurance information; 9) An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or 10) The individual's digitized or other electronic signature. § 51-30-01(4)(a)(1)-(10). “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. § 51-30-01(4)(b).
Definition of “Breach”	Unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable. § 51-30-01(1).
Analysis of Risk of Harm	Notification is required only if a resident’s encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. § 51-30-02.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Notification is not required when data has been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable. § 51-30-01(1).
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of the person is not a breach of the security of the system, if the personal information is not used or subject to further unauthorized disclosure. § 51-30-01(1).
Notification Obligation	Any person that owns or licenses computerized data that includes personal information, shall disclose any breach of the security system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. § 51-30-02. Notice under this chapter may be provided by one of the following methods: 1) Written notice; 2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of title 15 of the United States Code; or

	3) Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information. Substitute notice consists of the following: a. Electronic mail notice when the person has an electronic mail address for the subject persons; b. Conspicuous posting of the notice on the person's website page, if the person maintains one; and c. Notification to major statewide media. § 51-30-05.
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	Any person that experiences a breach of the security system as provided in this section shall disclose to the attorney general by mail or electronic mail any breach of the security system which exceeds 250 individuals. § 51-30-02.
Notification for Third-Party Data	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 the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. § 51-30-03.
Timing of Notification	The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system. § 51-30-02. The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this chapter must be made after the law enforcement agency determines that the notification will not compromise the investigation. § 51-30-04.
Private Cause of Action / Enforcement / Penalties	The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law. § 51-30-07.
Exceptions	Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. 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 in compliance with this chapter. A covered entity, business associate, or subcontractor subject to breach notification requirements under title 45, Code of Federal Regulations, subpart D, part 164, is considered to be in compliance with this chapter. § 51-30-06.
Other Key Provisions	N/A

State/Territory	**OHIO**
Statute	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192.

Definition of "Personal Information"	An individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: 1) Social security number; 2) Driver's license number or state identification card number; 3) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account. § 1349.19(A)(7)(a). "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 any of the following media that are widely distributed: 1) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television; 2) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in division (A)(7)(b)(i) of this section; 3) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation; 4) Any type of media similar in nature to any item, entity, or activity identified in division (A)(7)(b)(i), (ii), or (iii) of this section. § 1349.19(A)(7)(b).
Definition of "Breach"	Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state. § 1349.19(A)(1)(a). Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. § 1349.19(A)(1)(b)(i). Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach of the security of the system. § 1349.19(A)(1)(b)(ii).
Analysis of Risk of Harm	Notification is required only if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. § 1349.19(B)(1).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	If the data is encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable, notification is not required. § 1349.19(A)(7)(a).
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. § 1349.19(A)(1)(b)(i).
Notification Obligation	Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. § 1349.19(B)(1).

	A person may disclose or make a notification by any of the following methods: 1) Written notice; 2) Electronic notice, if the person's primary method of communication with the resident to whom the disclosure must be made is by electronic means; 3) Telephone notice; § 1349.19(E)(1)-(3). 4) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described in division (E)(1), (2), or (3) of this section, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed two hundred fifty thousand dollars, or that the affected class of subject residents to whom disclosure or notification is required exceeds five hundred thousand persons. Substitute notice under this division shall consist of all of the following: a. Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made; b. Conspicuous posting of the disclosure or notice on the person's web site, if the person maintains one; c. Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds seventy-five per cent of the population of this state. § 1349.19(E))(4). 5) Substitute notice, if the person required to disclose demonstrates that the person is a business entity with ten employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed ten thousand dollars. Substitute notice under this division shall consist of all of the following: a. Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the business 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; b. Conspicuous posting of the disclosure or notice on the business entity's web site, if the entity maintains one; c. Notification to major media outlets in the geographic area in which the business entity is located. § 1349.19(E)(5).
Notification to Consumer Reporting Agencies	If a person discovers circumstances that require disclosure under this section to more than one thousand residents of this state involved in a single occurrence of a breach of the security of the system, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the person to the residents of this state. In no case shall a person that is required to make a notification required by this division delay any disclosure or notification in order to make the notification required by this division. § 1349.19(G).
Notification to Regulators	N/A
Notification for Third-Party Data	Any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes personal information shall notify that other person or governmental entity of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state. § 1349.19(C).
Timing of Notification	The person shall make the disclosure in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system. § 1349.19(B)(2).

	The person may delay the disclosure or notification if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security. § 1349.19(D).
Private Cause of Action / Enforcement / Penalties	The attorney general may conduct pursuant to sections 1349.191 and 1349.192 of the Revised Code an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of this section. § 1349.19(I).
Exceptions	A financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, 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 for compliance with the applicable federal law, is exempt from the notification requirements. § 1349.19(F)(1).
Other Key Provisions	Any waiver is contrary to public policy and is void and unenforceable. § 1349.19(H). Section 1347.12 governs agency disclosure of security breach of computerized personal information data and nearly mirrors the above provisions. Sections 1349.191-192 govern the attorney general's investigative and enforcement authority related to noncompliance with the above provisions.

State/Territory	**OKLAHOMA**
Statute	24 Okla. Stat. §§ 161–66.
Definition of “Personal Information”	First name or first initial and last name in combination with one or more of the following data elements if the elements are neither encrypted nor redacted, or are encrypted or redacted but the keys to unencrypt or unredact were acquired without authorization in the breach: (1) social security number; (2) driver’s license number or state identification card number; or (3) account number or credit/debit card number in combination with any required security/access code or password that permits access to the consumer’s financial account. § 24-162(3), (6).
Definition of “Breach”	Unauthorized access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an entity as part of a database of personal information regarding multiple individuals <u>that causes, or the individual or entity reasonably believes has caused or will cause</u>, identity theft or fraud to any Oklahoma resident. Good faith exceptions exist for the data collector’s agents or employees. § 24-162(1).
Analysis of Risk of Harm	Notice is required if the individual or entity reasonably believes that the misuse of personal information has caused or will cause identity theft or fraud to an Oklahoma resident. § 24-162(1), § 24-163(B).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	If the personal information is encrypted, redacted, unreadable, or unusable, then a breach has not occurred provided the encryption key was not acquired. § 24-162(3), (6).
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity subject to further unauthorized disclosure. § 24-162(1).
Notification Obligation	An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state 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 this state. § 24-163(A). An individual or entity must give notification by (1) written notice; (2) telephonic notice; (3) electronic notice; or (4) substitute notice, if (a) the cost will exceed $50,000; (b) the number of affected consumers to receive notice exceeds 100,000; or (c) the person lacks sufficient contact information to provide notice, then the person will provide substitute notice through <u>at least two</u> of the following: (i) emails if the person has them for this class of consumer; (ii) conspicuous posting on the entity’s website (if the entity has a website); and (iii) notice to major statewide media. § 24-162(7).

	The statute does not explicitly require that electronic notice be consistent with 15 U.S.C. § 7001. § 24-162(7).
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	If the person is subject to the state Real Estate Commission, then the person must notify the Commission. Okla. Admin. Code § 605:10-13-1.
Notification for Third-Party Data	If entity maintains personal information on behalf of another, then the individual or entity must notify the owner or licensee of the information of any breach if personal information was or is reasonably believed to have been accessed or acquired by an unauthorized person. § 24-163(C).
Timing of Notification	Without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and restore the computerized data system's reasonable integrity, security, and confidentiality. § 24-163(A).
Private Cause of Action / Enforcement / Penalties	Private Cause of Action: No. The AG or district attorney has exclusive authority to bring actions for violations of this statute and civil penalties can reach $150,000 per breach or series of breaches discovered in a single investigation. § 24-165(B). Violations of this Act resulting in injury or loss may also violate the Oklahoma Consumer Protection Act and subject the entity to action by the AG or a district attorney. § 24-165(A).
Exceptions	Delayed Notification: When requested by law enforcement or as necessary to determine the scope of the breach and restore reasonable integrity of the computerized data system. § 24-163(D). Own Notification Procedures: If a person's own notification procedures, as part of an information security policy for personal information treatment, are consistent with Oklahoma's notification timing requirements, then the person does not violate this section if the person notifies consumers in accordance with its policies in the event of a breach. § 24-164. Financial Institutions: • Violations by a state-chartered or state-licensed financial institution shall be enforceable exclusively by the primary state regulator of the financial institution. • Compliance with the notification requirements of the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed as compliance with this Act. § 24-164(B)(1). Federal Regulator Compliance: Compliance with the procedures of an entity's primary or functional federal regulator shall be deemed compliance with this Act. § 24-164(B)(2).
Other Key Provisions	N/A

State/Territory	**OREGON**
Statute	Or. Rev. Stat. §§ 646A.600-604.
Definition of "Personal Information"	A consumer's first name or first initial and last name in combination with any one or more of the following data elements, 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 state identification card number issued by the Department of Transportation; • Passport number or other ID number issued by the United States; • Financial account number, credit card number, or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account; • Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina, or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction; • Health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or • Any information about medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; § 646A.602(12)(a)(A). 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. § 646A.602(12)(a)(B). Any of the data elements described above constitute personal information if they are without the consumer's first name or first initial and last name and if encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and the data element or combination of data elements would enable a person to commit identity theft against a consumer. §646A.602(12)(a)(C). Information in a federal, state or local government record, other than a Social Security number, that is lawfully made available to the public is not included. § 646A.602(12)(b).
Definition of "Breach"	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information that a person maintains or possesses. § 646A.602(1)(a).
Analysis of Risk of Harm	A covered entity 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 entity must document the determination in writing and maintain the documentation for at least five (5) years. § 646A.604(8).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	No notification is required if personal information is unusable due to encryption, redaction, or other methods. § 646A.602(12).

Unauthorized Employee Disclosure	Breach does not include an inadvertent acquisition of personal information by a person or the person's employee or agent if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information. § 646A.602(1)(b).
Notification Obligation	If a covered entity is subject to a breach of security or receives notice of a breach of security from a vendor, the covered entity shall give notice of the breach to the consumer to whom the personal information pertains, and the Attorney General. § 646A.602(5), § 646A.604(1)(a). Notice must include, at minimum: a description of the breach of security in general terms; the approximate date of the breach of security; the type of personal information that was subject to the breach of security; contact information for the covered entity; contact information for national consumer reporting agencies; and advice to the individual to report suspected identity theft to law enforcement, including the Oregon Attorney General and the Federal Trade Commission. § 646A.604(5). Notice may be provided by any of the following methods: in writing; electronically, if the covered entity customarily communicates with the consumer electronically or if the notice is consistent with 15 U.S.C. § 7001; by telephone if the affected person is contacted directly; or by substitute notice of the cost of notification otherwise would exceed $250,000 if the affected class of consumers exceeds 350,000, or if there insufficient contact information to notify affected persons. § 646A.604(4).
Notification to Consumer Reporting Agencies	When a covered entity discovers or received notice of a breach of security affecting more than one thousand (1,000) individuals that requires disclosure, the covered entity shall notify, without unreasonable delay, all consumer-reporting agencies that compile and maintain reports on individuals on a nationwide basis of the timing, distribution, and content of the notification given by the covered entity to the individuals. The covered entity shall include the police reporting number, if available, in its notification to the consumer reporting agencies. § 646A.604(6).
Notification to Regulators	If a covered entity is subject to a breach of security or receives notice of a breach of security from a vendor, the covered entity shall give notice of the breach to the Attorney General, either in writing or electronically, if the number of consumers to whom the covered entity must send the notice to exceeds 250. § 646A.602(5), § 646A.604(1)(b). Entities that are otherwise exempt from the statute's requirements must provide to the Oregon Attorney General within a reasonable time at least one copy of any notice the person sends to consumers or to the person's primary or functional regulator in compliance with this section or with other state or federal laws or regulations that apply to the person as a consequence of a breach of security. § 646A.604(10).
Notification for Third-Party Data	(a) 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. (b) If a vendor has a contract with another vendor that, in turn, has a contract with a covered entity, the vendor shall notify the other vendor of a breach of security as provided in paragraph (a) of this subsection. (c) 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. This paragraph does not apply to the vendor if the covered entity described in paragraph (a) or (b) of this subsection has notified the Attorney General in accordance with the requirements of this section. § 646A.604(2)(a)-(c).
Timing of Notification	The covered entity shall notify the consumer in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notice of the breach, but must undertake reasonable measures necessary to determine sufficient contact information for the affected consumer, the scope of the breach of security, and restore the reasonable integrity, security and confidentiality of the personal information before providing notice. § 646A.604(3)(a), (b).

	A person that must give notice of a breach of security under this section may delay giving the notice only if a law enforcement agency determines that a notification will impede a criminal investigation and if the law enforcement agency requests in writing that the person delay the notification. § 646A.604(3)(c).
Private Cause of Action / Enforcement / Penalties	A person's violation of a provision of this statute is an unlawful practice under Or. Rev. Stat. § 646.607 [Unlawful Trade Practice]. The rights and remedies under this section are cumulative and are in addition to any other rights and remedies that are available under law. § 646A.604(11). (b) A covered entity or vendor in an action or proceeding may affirmatively defend against an allegation that the covered entity or vendor has not developed, implemented and maintained reasonable safeguards to protect the security, confidentiality and integrity of personal information that is subject to ORS 646A.600 to 646A.628 but is not subject to an Act described in subsection (9)(c) or (d) of this section by showing that, with respect to the personal information that is subject to ORS 646A.600 to 646A.628, the covered entity or vendor developed, implemented and maintained reasonable security measures that would be required for personal information subject to the applicable Act. § 646A.604(11)(b).
Exceptions	This section does not apply to: (1) 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, if the personal information and the person would otherwise be subject to ORS 646A.600 to 646A.628. § 646A.604(9)(A). (2) 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 section. § 646A.604(9)(B). (3) A covered entity or vendor that complies with regulations promulgated under Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) as that Act existed on January 1, 2020, if personal information that is subject to ORS 646A.600 to 646A.628 is also subject to that Act. § 646A.604(9)(C). (4) A covered entity or vendor that complies with regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, 110 Stat. 1936) and the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5, Title XIII, 123 Stat. 226), as those Acts existed on January 1, 2020, if personal information that is subject to ORS 646A.600 to 646A.628 is also subject to those Acts. § 646A.604(9)(D).
Other Key Provisions	A "covered entity" means a person that owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses personal information in the course of the person's business, vocation, occuptation or volunteer activities. § 646A.602(5)(a). A "covered entity" does not include a person described in paragraph (a) of this subsection to the extent that the person acts solely as a vendor. § 646A.602(5)(b).

State/Territory	**PENNSYLVANIA**
Statute	73 Pa. Stat. § 2301, *et seq*.
Definition of "Personal Information"	First name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (1) Social Security number; (2) driver's license number or state ID card number issued in lieu of a driver's license; or (3) 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. § 2302. The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records. § 2302.
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 part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to a Pennsylvania resident. § 2302.
Analysis of Risk of Harm	Notice of any breach of the security of the system is required following discovery of the breach of the security of the system if the unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. § 2303(a).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Notification is not required when encrypted or redacted information is accessed and acquired. It is only required when the information is in an unencrypted form or if the security breach involves a person with access to the encryption key. § 2303(b).
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure. § 2302.
Notification Obligation	Any entity to which the statute applies shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any individual whose principal mailing address, as reflected in the computerized data that is maintained, stored, or managed by the entity, is in PA whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. § 2303(a).
Notification to Consumer Reporting Agencies	When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and number of notices. § 2305.
Notification to Regulators	N/A

Notification for Third-Party Data	A vendor that maintains, stores, or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery to the entity on whose behalf it maintains, stores or manages the data. § 2303(c).
Timing of Notification	Notice shall be made without unreasonable delay. § 2303(a). Notification may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. Notification shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security. § 2304.
Private Cause of Action / Enforcement / Penalties	A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of 73 Pa. Stat. § 201-1 *et seq.* known as the Unfair Trade Practices and Consumer Protection Law. **Attorney General Enforcement:** The Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of the statute. § 2308.
Exceptions	**Own Notification Policy:** An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security. § 2307(a). **Compliance with Other Laws:** • **Compliance with Primary Regulator.** An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional federal regulator shall be in compliance with this act. § 2307(b)(2). • **Federal Interagency Guidance.** 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 with this act. § 2307(b)(1).
Other Key Provisions	This statute shall supersede and preempt all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities and other local agencies within this Commonwealth regarding the matters expressly set forth in this statute. § 2306.

State/Territory	**PUERTO RICO**
Statute	P.R. Laws tit. 10, §§ 4051, *et seq.*
Definition of "Personal Information"	"Personal information file" means a file containing at least the name or first initial and the surname of a person, together with any of the following data 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: i. Social security number; ii. Driver's license number, voter's identification or other official identification iii. Bank or financial account numbers of any type with or without passwords or access code that may have been assigned; iv. Names of users and passwords or access codes to public or private information systems; v. Medical information protected by the HIPAA; vi. Tax information; or vii. Work-related evaluations. § 4051(a). Neither the mailing nor the residential address is included in the protected information or information that is a public document and that is available to the citizens in general. § 4051(a).
Definition of "Breach"	"Violation of the security system" means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings. § 4051(c).
Analysis of Risk of Harm	Notification is required when it is known or there is reasonable suspicion that persons or entities have violated this statute. § 4051(c).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Personal information that requires a special cryptographic code is not personal information. § 4051(a).
Unauthorized Employee Disclosure	N/A
Notification Obligation	Any entity that is the proprietor or custodian of a database for commercial use that includes personal information of citizens who reside in Puerto Rico must notify said citizens of any breach of the security of the system when the database whose security has been breached contains, in whole or in part, personal information files and the same are not protected by an encrypted code but only by a password.

	Any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons. § 4052. The notice of breach of the security of the system shall be submitted in a clear and conspicuous manner and should describe the breach of the security of the system in general terms and the type of sensitive information compromised. The notification shall also include a toll free number and an Internet site for people to use in order to obtain information or assistance. The notification can be made by any of the following methods: • written direct notice to those affected by mail or by authenticated electronic means according to the Digital Signatures Act. • when the cost of notifying all those potentially affected or of identifying them is excessively onerous due to the number of persons affected, to the difficulty in locating all persons or to the economic situation of the enterprise or entity; or whenever the cost exceeds one hundred thousand dollars ($100,000) or the number of persons exceeds one hundred thousand ($100,000), the entity shall issue the notice through the following two (2) steps: (i) prominent display of an announcement to that respect at the entities 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 (ii) a communication to that respect to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector. § 4053.
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	The parties responsible shall inform the Department of Consumer Affairs within ten days, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information. § 4052.
Notification for Third-Party Data	Any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons. § 4052.
Timing of Notification	Residents must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security. Within a non-extendable term of ten days after the violation of the system's security has been detected, the parties responsible shall inform the Department of Consumer Affairs, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information. § 4052.
Private Cause of Action / Enforcement / Penalties	The Secretary may impose fines of $500 up to a maximum of $5,000 for each violation of the provisions of this chapter or its regulations. The fines provided in this section do not affect the rights of the consumers to initiate actions or claims for damages before a competent court. § 4055.
Exceptions	No provision of this law shall be interpreted as being prejudicial to those institutional information and security policies that an enterprise or entity may have in force prior to its effectiveness and whose purpose is to provide protection equal or better to the information on security herein established. § 4054.

Other Key Provisions	In those cases in which the breach or irregularity in the security systems of the database occurs in a government agency or public corporation, it shall be notified to the Citizen's Advocate Office, which shall assume jurisdiction. For this purpose, the Citizen's Advocate shall designate a Specialized Advocate who shall address these types of cases. § 4054a.

State/Territory	**RHODE ISLAND**
Statute	R.I. Gen. Laws §§ 11-49.3-1 to 11.49.3-6.
Definition of “Personal Information”	An individual’s first name or first initial and last name plus any one or more of the following data elements (when the name and the data elements are not encrypted or are in hard copy, or paper format): (1) Social Security number; (2) Driver’s license number, Rhode Island identification card number, or tribal identification number; (3) Account number, credit or debit card number, in combination with any required security code, access code, password, or personal identification number, that would allow access to an individual’s financial account; (4) Medical or health insurance information; (5) E-mail address with any required security code, access code, or password that would allow access to an individual’s personal, medical, insurance or financial account. § 11-49.3-3(a)(8).
Definition of “Breach”	Unauthorized access or acquisition of unencrypted, computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency, or person. There is a good-faith exception for the acquisition of personal information by an employee or agent of the agency for the purposes of the agency. § 11-49.3-3(a)(1).
Analysis of Risk of Harm	Notification is not required if the breach or disclosure of personal information does not pose a significant risk of identity theft to any resident of Rhode Island. § 11-49.3-4(a)(1).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	If the information is encrypted, notification is not required. Information that is acquired in combination with a key, security code, or password that would permit access to the data is not considered encrypted. § 11-49.3-3(a)(2).
Unauthorized Employee Disclosure	Good-faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. § 11-49.3-3(a)(1).
Notification Obligation	Any entity who owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information must provide notification of any disclosure of personal information or breach of the security system that poses a significant risk of identity theft to any Rhode Island resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity. § 11-49.3-4(a)(1).
Notification to Consumer Reporting Agencies	If more than 500 Rhode Island residents are to be notified, the entity must also notify the major Credit Reporting Agencies of the timing, content, and distribution of the notices and the approximate number of affected individuals. This notice must be made without delaying notice to the affected Rhode Island residents. § 11-49.3-4(a)(2).
Notification to Regulators	If more than 500 Rhode Island residents are to be notified, the entity must also notify the Attorney General of the timing, content, and distribution of the notices and the approximate number of affected individuals. This notice must be made without delaying notice to the affected Rhode Island residents. § 11-49.3-4(a)(2).
Notification for Third-Party Data	An entity who or that discloses personal information about a Rhode Island resident to a nonaffiliated third party shall require by written contract that the third party implement and maintain reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure. The provisions of this section shall apply to contracts entered into after the effective date of this act. § 11-49.3-2(b).

Timing of Notification	Notification must be made in the most expedient time possible, but no later than forty-five (45) days after confirmation of the breach and after ascertaining the information required to fulfil the notice requirements and consistent with the needs of law enforcement. Notification may be delayed if a law enforcement agency determines that notification will impede a criminal investigation. Once the law enforcement agency determines that notification will no longer compromise a criminal investigation, notice should be given as soon as practicable. § 11-49.3-4(a)(2)(b).
Private Cause of Action / Enforcement / Penalties	Every reckless violation of this chapter is a civil violation. A penalty of not more than one hundred dollars ($100) per record may be charged against the violator. Every knowing and willful violation of this chapter is a civil violation. A penalty of not more than two hundred dollars ($200) per record may be charged against the violator. If the Attorney General has reason to believe that a violation occurred, and that proceedings are in the public interest, the Attorney General has a right to bring an action in the name of the state against the business or person in violation. § 11-49.3-5.
Exceptions	The following agencies or persons with its own security breach procedures are deemed to be in compliance with the security breach notification requirements: (1) An entity that maintains its own security breach procedures as part of an information security policy for treatment of personal information and follows the notification requirements of this chapter, and notifies the affected persons in accordance with its policies; (2) An entity that maintains a breach procedure based on the rules, regulations, procedures, or guidelines established by the primary or functional regulator and notifies the affected person in accordance with the primary or functional regulator; (3) A financial institution, trust company, credit union, or its affiliates that is subject to and found in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to customer Information and Customer Notice; (4) A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the Federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPPA). § 11-49.3-6.
Other Key Provisions	An entity who or that stores, collects, processes, maintains, acquires, uses, owns, or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information. § 11-49.3-2(a). A entity shall not retain personal information for a period longer than is reasonably required to provide the services requested; to meet the purpose for which it was collected; or in accordance with a written retention policy or as may be required by law. A municipal agency, state agency, or person shall destroy all personal information, regardless of the medium that such information is in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or erasure. § 11-49.3-2(a).

State/Territory	**SOUTH CAROLINA**
Statute	S.C. Code Ann. § 39-1-90.
Definition of "Personal Information"	"Personal identifying information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted: (a) Social security number; (b) Driver's license number or state identification card number issued instead of a driver's license; (c) 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 a resident's financial account; or (d)Oother numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual. The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local governmental records lawfully made available to the general public. § 39-1-90(D)(3).
Definition of "Breach"	Unauthorized access and acquisition of computerized data that was not encrypted, redacted, or otherwise secured, 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. Good faith acquisition of personal identifying information by a business for the purposes of its business is not a breach if the personal identifying information is not used or subjected to further unauthorized disclosure. § 39-1-90(D)(1).
Analysis of Risk of Harm	Any entity to which the statute applies shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of SC whose unencrypted and unredacted personal information, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information **has occurred or is reasonably likely to occur or use the information creates a material risk of harm** to the resident. § 39-1-90(D)(1).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	If data is rendered unusable through encryption, redaction, or other methods, notice to consumers is not required. § 39-1-90(D)(1).
Unauthorized Employee Disclosure	Good faith acquisition of personal identifying information by a business for the purposes of its business is not a breach if the personal identifying information is not used or subjected to further unauthorized disclosure. § 39-1-90(D)(1).
Notification Obligation	Notification may be provided by: • Written notice • Electronic notice if the person's primary method of communication with the individual is by electronic means • Telephonic notice

	Substitute notice if the person demonstrates that the cost of providing notice exceeds $250,000 or that the affected class of subject persons to be notified exceeds $500,000, or the person has sufficient contact information (substitute notice may be given by email, conspicuous posting of the notice on the website of the person, if one is maintained). § 39-1-90(E).
Notification to Consumer Reporting Agencies	If 1,000 or more persons are affected, the entity shall notify, without unreasonable delay, the Consumer Protection Division and the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on a nationwide basis of the timing, distribution, and content of the notice. § 39-1-90(K).
Notification to Regulators	N/A
Notification for Third-Party Data	A person conducting business in the state and maintaining computerized or other personal information data that the person does not own shall notify the owner or licensee of the information in case of a breach immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person. § 39-1-90(B).
Timing of Notification	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. § 39-1-90(A).
Private Cause of Action / Enforcement / Penalties	A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may: (1) institute a civil action to recover damages in case of a willful and knowing violation; (2) institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section; (3) seek an injunction to enforce compliance; and (4) recover attorney's fees and court costs, if successful. § 39-1-90(G). A person who knowingly and willfully violates this section is subject to an administrative fine in the amount of $1,000 for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs. § 39-1-90(H).
Exceptions	**Own Notification Policy**: An entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise 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 subject persons in accordance with its policies in the event of a breach of security of the system. § 39-1-90(F). **Gramm-Leach-Bliley Act**: This breach section does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provisions of the Gramm-Leach-Bliley Act. § 39-1-90(I). **Interagency Guidance**: A financial institution that is subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as amended, is considered to be in compliance with this section. § 39-1-90(J).
Other Key Provisions	**Delay for Law Enforcement**: The notification required by the statute may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification must be made once law enforcement determines it would no longer compromise the investigation. § 39-1-90(C).

State/Territory	**SOUTH DAKOTA**
Statute	S.D. Codified Laws §§ 22-40-19 to 22-40-26.
Definition of “Personal Information”	A person’s first name or first initial and last name, in combination with any one or more of the following data elements: (1) Social Security number; (2) driver’s license number or other unique identification number created or collected by a government body; (3) account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person’s financial account; (4) health information as defined in 45 CFR 160.103 (HIPAA); or (5) an identification number assigned to a person by the person’s employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes. § 22-40-19(4). The Act also covers breaches of “protected information,” which includes: (1) a user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and (2) account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person’s financial account. § 22-40-19(5).
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 information holder. The term does not include the good faith acquisition of personal or protected information by an employee or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure. § 22-40-19(1).
Analysis of Risk of Harm	An information holder is not required to make a disclosure to an affected person if, following an appropriate investigation and notice to the Attorney General, the information holder reasonably determines that the breach will not likely result in harm to the affected person. The information holder must document the determination in writing and maintain the documentation for not less than 3 years.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	As long as the personal information is redacted or encrypted and the encryption key was not accessed or acquire. § 22-40-19(1), (4).
Unauthorized Employee Disclosure	A breach does not include the good faith acquisition of personal or protected information by an employee or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure. § 22-40-19(1).
Notification Obligation	Following the discovery by or notification to an information holder of a breach of system security an information holder shall disclose in accordance with § 22-40-22 the breach of system security to any resident of this state whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person. § 22-40-20. Notice may be provided by (1) written notice; (2) electronic notice, if the electronic notice is consistent with 15 U.S.C § 7001, or if the information holder’s primary method of communication with the resident of this state has been by electronic means; or (3) substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, that the affected class of persons to be notified exceeds five hundred thousand persons, or that the information holder does not have sufficient contact information and the notice consists of each of the following: (a) email notice, if the information holder has an email

	address for the subject persons; (b) conspicuous posting of the notice on the information holder's website, if one is maintained; and (c) notification to statewide media. § 22-40-22.
Notification to Consumer Reporting Agencies	The information holder must notify, without reasonable delay, all consumer reporting agencies and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis. § 22-40-24.
Notification to Regulators	Any information holder that experiences a breach of system security under this section shall disclose to the attorney general by mail or electronic mail any breach of system security that exceeds 250 residents of this state. § 22-40-20.
Notification for Third-Party Data	N/A
Timing of Notification	A disclosure under this section shall be made not later than 60 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. § 22-40-20.
Private Cause of Action / Enforcement / Penalties	The state attorney general may prosecute each failure to disclose under the provisions of this Act as a deceptive act or practice under S.D. Codified Law (SDCL) § 37-24-6 and, in addition to any remedy provided for such acts or practices, may bring an action on behalf of the state to recover a civil penalty of up to ten thousand dollar per day, per violation. The attorney general also may recover attorney's fees and costs associated with bringing such an enforcement action. § 22-40-25.
Exceptions	An information holder that maintains its own notification procedure as part of its information security policy, and the policy is consistent in compliance with the notification requirements of this Act if it notifies affected persons in accordance with its internal policy. § 22-40-23. Any information holder that is regulated by federal law or regulation, including HIPAA or the Gramm Leach Bliley Act and that maintains procedures for a breach of system security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional federal regulator is deemed to be in compliance with this chapter if the information holder notifies affected South Dakota residents in accordance with the provisions of the applicable federal law or regulation. § 22-40-26.
Other Key Provisions	Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, the notification shall be made not later than 30 days after the law enforcement agency determines that notification will not compromise the criminal investigation. § 22-40-21.

State/Territory	**TENNESSEE**
Statute	Tenn. Code. Ann. § 47-18-2107.
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: (1) Social Security number; (2) driver license number; or (3) account, credit card, 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. The definition does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted or otherwise made unusable. § 47-18-2107(a)(4).
Definition of "Breach"	The acquisition of personal information by an unauthorized person (including an employee of the information holder who is discovered by the information holder to have obtained personal information with the intent to use it for an unlawful purpose) that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder; unencrypted computerized data; or encrypted computerized data and the encryption key. A breach does not include the good faith acquiring of personal information by an employee or agent of the information holder for the purposes of the information holder if the personal information is not used or subject to further unauthorized disclosure. § 47-18-2107(a)(1).
Analysis of Risk of Harm	Notice must be given to any resident of Tennessee whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. § 47-18-2107(b).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The statute does not apply to information that has been redacted or otherwise made unusable or indecipherable. § 47-18-2107(a)(2).
Unauthorized Employee Disclosure	The term "unauthorized person" includes an employee of the information holder who is discovered by the information holder to have obtained personal information with the intent to use it for an unlawful purpose. § 47-18-2107(a)(5).
Notification Obligation	Following discovery or notification of a breach of system security by an information holder, the information holder (any person or business that conducts business in Tennessee, or any agency of Tennessee or any of its political subdivisions, that owns or licenses computerized personal information of residents of Tennessee) shall disclose the breach of system security to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. § 47-18-2107(b). Notice may be provided by one of the following methods: (1) Written notice;(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the E-SIGN Act [15 U.S.C. § 7001] or if the information holder's primary method of communication with the resident of this state has been by electronic means; or (3) By substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred and fifty thousand dollars ($250,000), that the affected class of subject persons to be notified exceeds five hundred thousand (500,000) persons, or the information holder does not have sufficient contact information. Substitute notice must consist of all of the following: email notice, when the information holder has an email address for the subject persons; Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and Notification to major statewide media. § 47-18-2107(e).

Notification to Consumer Reporting Agencies	If an information holder discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one time, the information holder must also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. § 1681a, and credit bureaus that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. § 47-18-2107(g).
Notification to Regulators	N/A
Notification for Third-Party Data	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. § 47-18-2107(c).
Timing of Notification	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. § 47-18-2107(b).
Private Cause of Action / Enforcement / Penalties	Private Right of Action: Any customer of an information holder who is a person or business entity, but who is not an agency of this state or any political subdivision of this state, and who is injured by a violation of this section, may institute a civil action to recover damages and to enjoin the information holder from further action in violation of this section. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law. § 47-18-2107(h). A violation constitutes a violation of the Tennessee Consumer Protection Act. § 47-18-2106. Notwithstanding any other law, a violation of this part shall be punishable by a civil penalty of whichever of the following is greater: $10,000, $5,000 per day for each day that a person's identity has been assumed or 10 times the amount obtained or attempted to be obtained by the person using the identity theft. This civil penalty is supplemental, cumulative, and in addition to any other penalties and relief available under the Tennessee Consumer Protection Act, or other laws, regulations or rules. § 47-18-2106.
Exceptions	Own Notification Policy: If an information holder maintains its own notification procedures as part of an information security policy for the treatment of personal information and if the policy is otherwise consistent with the timing requirements of this section, the information holder is in compliance with the notification requirements of this section, as long as the information holder notifies subject persons in accordance with its policies in the event of a breach of system security. § 47-18-2107(f). Delayed Notification: The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, it must be made no later than 45 days after the law enforcement agency determines that notification will not compromise the investigation. § 47-18-2107(d). Other Laws: This section does not apply to any information holder that is subject to: (1) Title V of the Gramm-Leach-Bliley Act of 1999 (Pub. L. No. 106-102); or (2) The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d *et seq.*), as expanded by the Health Information Technology for Clinical and Economic Health Act (42 U.S.C. § 300jj *et seq.*, and 42 U.S.C. § 17921 *et seq.*). § 47-18-2107(i).

Other Key Provisions	Application: The statute applies to any "information holder," meaning any person or business that conducts business in this state, or any agency of this state or any of its political subdivisions, that owns or licenses computerized personal information of residents of Tennessee. § 47-18-2107(a)(3).

State/Territory	**TEXAS**
Statute	Tex. Bus. & Com. Code Ann. §§ 521.002, 521.053, 521.151.
Definition of "Personal Information"	"Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including (A) an individual's: name, social security number, date of birth, or government-issued identification number; (B) mother's maiden name; (C.) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (D) unique electronic identification number, address, or routing code; and (E) telecommunication access device as defined by Section 32.51, Penal Code. .§ 521.002(1). "Sensitive personal information" means (A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) 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; or (B) information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.§ 521.002(2).
Definition of "Breach"	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. Good faith exceptions exist for the person's agents or employees. § 521.053(a).
Analysis of Risk of Harm	Must report to any individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person. § 521.053(b).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	If the data is encrypted and the encryption key was not accessed or acquired. § 521.053(a).
Unauthorized Employee Disclosure	Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner. § 521.053(a).
Notification Obligation	A person who conducts business in Texas and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system or at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.§ 521.053(b). A person may give notice by providing: (1) written notice at the last known address of the individual; electronic notice, if the notice is provided in accordance with 15 U.S.C. § 7001; or (3) substitute notice, if the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not

	have sufficient contact information. Substitute notice may be given by (a) email, (b) conspicuous posting on the person's website, or (3) notice published in a broadcast on major statewide media. § 521.053(e), (f).
Notification to Consumer Reporting Agencies	If a breach in this section requires notifying more than 10,000 people at one time, then the person must also notify a nationwide consumer reporting agency without unreasonable delay. § 521.053(h).
Notification to Regulators	If the breach involves at least 250 Texas residents, then the person must notify the Texas attorney general no later than 60 days after the date on which the person determines that the breach occurred, and this notification must include: • A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach; • The number or Texas residents affected at the time of notification; • The measures taken regarding the breach; • Any measure intended to be taken after notification; and • Information on whether law enforcement is investigating the breach. § 521.053(i).
Notification for Third-Party Data	If an entity maintains sensitive personal information on behalf of an owner or licensee, then the entity must notify them of a breach. § 521.053(c).
Timing of Notification	Notification should be made without unreasonable delay and no later than 60 days after the date on which the person determines that the breach occurred unless a delay is (1) at the request of law enforcement or (2) necessary to determine the scope of the breach and restore reasonable integrity of the data system. In the former case the notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation. § 521.053(b).
Private Cause of Action / Enforcement / Penalties	Civil Penalties: Injunctive relief and damages—at least $2,000 but not more than $50,000 for each violation. § 521.151(a). Additional Penalties: Failure to comply reasonably with the notification requirements may subject the entity to additional civil penalties of not more than $100 per individual that should have been notified per day up to a cap of $250,000. The attorney general may bring an action to recover these penalties. § 521.151(a-1).
Exceptions	Delayed Notification: A person may delay notification at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation. § 521.053(d). Own Notification Procedures: If a person's own notification procedures, as part of an information security policy for PI treatment, are consistent with Texas's notification timing requirements, then the person does not violate this section if the person notifies consumers in accordance with its policies in the event of a breach. § 521.053(g).
Other Key Provisions	If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person to provide notice of a breach of system security, the notice of the breach of system security required under Texas may be provided under that state's law or under Texas law. § 521.053(b-1).

State/Territory	**UTAH**
Statute	Utah Code Ann. §§ 13-44-101, and 13-44-202.
Definition of “Personal Information”	A person’s first name or first initial and last name, combined with any one or more 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; a financial account number, or credit or debit card number, and any required security code, access code, or password that would permit access to the person’s account; or driver license number or state identification card number. Personal information does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public. § 13-44-102(4).
Definition of “Breach”	An unauthorized acquisition of computerized date maintained by a person that compromises the security, confidentiality, or integrity of personal information. § 13-44-102(1).
Analysis of Risk of Harm	Notification is required if the investigation reveals that the misuse of personal information for identity theft or fraud purposes has occurred or is reasonably likely to occur. § 13-44-202(1)(b).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	No notification is required for the breach of information that is encrypted or protected by another method that renders the data unreadable or unusable. § 13-44-102(4)(a).
Unauthorized Employee Disclosure	"Breach of system security" does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner. § 13-44-202(1)(a).
Notification Obligation	A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes. If an investigation reveals that the misuse of personal information for identify theft or fraud purposes has occurred or is reasonably likely to occur, the person shall provide notification to each affected Utah resident. § 13-44-202(1). A notification required by this section may be provided: (i) In writing by first-class mail to the most recent address the person has for the resident; (ii) Electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001; (iii) By telephone, including through the use of automatic dialing technology not prohibited by other law; or (iv) For residents of the state for whom notification in a manner described in Subsections (5)(a)(i) through (iii) is not feasible, by publishing notice of the breach of system security: (A) in a newspaper of general circulation; and (B) as required in Section 45-1-101. § 13-44-202(5).
Notification to Consumer Reporting Agencies	N/A

Notification to Regulators	N/A
Notification for Third-Party Data	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. § 13-44-202(3)(a).
Timing of Notification	A person required to provide notification shall provide the notification in the most expedient time possible without unreasonable delay: (a) considering legitimate investigative needs of law enforcement, (b) after determining the scope of the breach of system security; and (c) after restoring the reasonable integrity of the system. § 13-44-202(2).
Private Cause of Action / Enforcement / Penalties	There is no private right of action. The Utah Attorney General may enforce this law. § 13-44-301. A person who violates this statute is subject to a civil penalty of: (a) no greater than $2,500 for a violation or series of violations concerning a specific consumer; and (b) no greater than $100,000 in the aggregate for related violations concerning more than one consumer, unless the violations concern: (A) 10,000 or more consumers who are residents of the state; and (B) 10,000 or more consumers who are residents of other states; or (ii) The person agrees to settle for a greater amount. Additionally, the Utah Attorney General may seek, in an action brought under this chapter: (i) injunctive relief to prevent future violations of this chapter; and (ii) attorney fees and costs. § 13-44-301(3), (4).
Exceptions	Financial Institutions: The statute does not apply to financial institutions or their affiliates, as defined in 15 U.S.C. § 6809. § 13-44-103. Own Notification: If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information the person is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach. § 13-44-202(5)(b). Delayed Notification: A person may, however, delay providing notification to affected persons at the request of a law enforcement agency that determines that notification may impede a criminal investigation. A person who delays providing notification under this section shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency inform the person that notification will no longer impede the criminal investigation. § 13-44-202(4). Other Laws: A person who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach. § 13-44-202(5)(c).
Other Key Provisions	A waiver of this section is contrary to public policy and is void and unenforceable. § 13-44-202(6).

State/Territory	**VERMONT**
Statute	Vt. Stat. tit. 9 §§ 2430, 2435.
Definition of “Personal Information”	“Personally identifiable information” means a consumer’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: (1) Social Security number; (2) a driver’s license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction; (3) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; (4) passwords or personal ID numbers or other access codes for a financial account; (5) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; (6) genetic information; and (7) health records or records of a wellness program or similar program of health promotion or disease prevention; a health care professional’s medical diagnosis or treatment of the consumers; or a health insurance policy number. § 2430(10). This statute also protects “brokered personal information.” § 2430(1).
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 maintained by a data collector. This does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the information or credentials are not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure. § 2430(13). This statute also protects consumers from data broker security breaches. § 2430(5).
Analysis of Risk of Harm	No notice is required if misuse of personal information is not reasonably possible. § 2435(d)(1).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	As long as the encryption key was not accessed or acquired. § 2430(7).
Unauthorized Employee Disclosure	N/A
Notification Obligation	Notification is required if the data collector establishes that the misuse of personally identifiable information or login credentials is reasonably possible. If the data collector established it is not reasonably possible, it must provide a detailed explanation for said determination to the attorney general or the Department of Financial Regulation. § 2435(d)(1).

	If a data collector established that misuse of personally identifiable information or login credentials was not reasonably possible and subsequently obtains facts indicating that misuse of the personally identifiable information or login credentials has occurred or is occurring, the data collector shall provide notice of the security breach. § 2435(d)(2). If a security breach is limited to an unauthorized acquisition of login credentials for an online account other than an email account, the data collector shall provide notice to the consumer electronically or through (a) written notice mailed to the consumer's residence; (b) electronic notice for consumers who have a valid email address (with certain restrictions); or (c) telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message. §§ 2435(d)(3), § 2435(b)(6). The data collector shall also advise the consumer to take steps necessary to protect the online account. If a security breach is limited to an unauthorized acquisition of login credentials for an email account, the data collector shall provide notice through the email account in addition to one or more of the methods specified in provision (b)(6) or by clear and conspicuous notice delivered to the consumer online. § 2435(d)(4). A financial institution regulated by the Department of Financial Regulation shall notify the Department as soon as possible after it becomes aware of an incident involving unauthorized access to or use of personally identifiable information. § 2435(g)(3). Contents of Notice (if known by the data collector): (1) the incident in general terms; (2) type of personally identifiable information subject to the security breach; (3) general acts of the data collector to protect the personally identifiable information from further breach; (4) a telephone number, toll-free if available, that the consumer may call for further assistance; (5) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and (6) the approximate date of the breach. § 2435(b)(5).
Notification to Consumer Reporting Agencies	In the event a data collector provides notice to more than 1,000 consumers at one time, the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the Department of Banking, Insurance, Securities, and Health Care Administration. § 2435(c).
Notification to Regulators	Notice must be provided to the Attorney General or, if regulated by the Department of Financial Regulation under Title 8, to the Department. § 2435(b)(3).
Notification for Third-Party Data	Any data collector that maintains or possesses computerized data containing personally identifiable information or login credentials that the data collector does not own or license or any Entity that conducts business in VT that maintains or possesses records or data containing personally identifiable information that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in the statute. § 2435(b)(2).
Timing of Notification	Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system. § 2435(b)(1).
Private Cause of Action / Enforcement / Penalties	The attorney general and state's attorney shall have sole and full authority to investigate potential violations and to enforce, prosecute, obtain, and impose remedies for a violation. The attorney general may refer the matter to the state's attorney in an appropriate case. § 2435(h)(1).
Exceptions	A financial institution that is subject to the following guidance, and any revisions, additions, or substitutions relating to said interagency guidance shall be exempt from this section: (i) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Costumer Notice, issued on March 7th,

	2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; (ii) Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14th, 2005, by the National Credit Union Administration.§ 2435(g).
Other Key Provisions	Delay for Law Enforcement: The required notice to a consumer shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or homeland security interests, jeopardize public safety or national or homeland security interests. In the event law enforcement makes the request in a manner other than in writing, the Entity shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The Entity shall provide the required notice without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay. § 2435(b)(4)(a). Waiver is not permitted. § 2435(f).

State/Territory	**VIRGINIA**
Statute	Va. Code §§ 18.2-186.6; 32.1-127.1:05; 58.1-341.2
Definition of "Personal Information"	First name or first initial and last name in combination with and linked to any one or more of the following data elements, when the data elements are neither encrypted nor redacted: (1) Social Security number; (2) driver's license number or state ID card number issued in lieu of a driver's license number; (3) financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; (4) Passport number; (5) Military ID number. § 18.2-186.6(A). **Medical Information-Specific Statute** For an authority, board, bureau, commission, district or agency of the state or of any political subdivision of the state, or organizations, corporations, or agencies in the state supported wholly or principally by public funds, the state's Medical Information Breach Notification statute may apply. The statute applies to Medical information, but not HIPAA covered entities or business associates. "Medical information" means the first name or first initial and last name with any of the following data elements that relate to a resident of Virginia, when the data elements are neither encrypted nor redacted: (1) any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (2) an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. Medical Information does not include information that is lawfully obtained from publically available information, or from federal, state, or local government records lawfully made available to the general public. § 32.1-127.1:05(A).
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 Virginia. § 18.2-186.6(A). **Medical Information-Specific Statute** Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality or integrity of **medical information** maintained by an entity. Good faith acquisition of medical information by an entity for the purposes of the entity is not a breach provided that the medical information is not used for a lawful purpose or not subject to further unauthorized disclosure. § 32.1-127.1:05(A).
Analysis of Risk of Harm	Notice is required if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes <u>has caused or will cause, identity theft or another fraud</u> to any resident of Virginia.

Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The unauthorized acquisition of encrypted or redacted data, without access to the encryption key, does not trigger the notice requirement under this statute. § 18.2-186.6(C).
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure. § 18.2-186.6(A).
Notification Obligation	If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of Virginia, an entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any affected resident of Virginia. § 18.2-186.6(B). An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of Virginia. § 18.2-186.6(C). For health information, the entity must notify both the subject of the medical information and any affected resident of Virginia, if those are not the same person. § 32.1-127.1:05(B).
Notification to Consumer Reporting Agencies	In the event an entity provides notice to more than 1,000 persons at one time pursuant to the general security breach section, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1682(a)(p), of the timing, distribution, and content of the notice. § 18.2-186.6(E).
Notification to Regulators	Notice, without unreasonable delay, to the attorney general if any Virginia residents must be notified. Notice may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. § 18.2-186.6(B). Notice to the attorney general is required for any breach requiring notification to more than 1,000 individuals. § 18.2-186.6(C). An employer or payroll service provider that owns or licenses computerized data relating to income tax withheld shall notify the Attorney General without unreasonable delay after discovery of a breach of taxpayer identification information. For employers, only need report information regarding employees, not customers or other non-employees. The employer must provide the Attorney General with the name and federal employer ID number of the employer that may be affected by the breach. § 18.2-186.6(M). **Special language for tax return preparers (as defined in Va. Code § 58.1-302):** Any tax return preparer who prepares a Virginia individual’s income tax returns during a calendar year shall notify the Department of Taxation without unreasonable delay after the discovery or notification of unauthorized access and acquisition of unencrypted and unredacted return information that compromises the confidentiality of such information maintained by such signing income tax return preparer and that

	creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person and that causes, or such preparer reasonably believes has caused or will cause, identity theft or other fraud. § 58.1-341.2(B)(1). **Medical Information-Specific Statute** If the entity provides notice to more than 1,000 persons at one time it must notify, without unreasonable delay, the attorney general and the Commissioner of Health of the timing, distribution, and content of the notice sent to affected persons. § 32.1-127.1:05(E).
Notification for Third-Party Data	An entity that maintains computerized data that includes personal information that the entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the entity reasonably believes the personal information was accessed and acquired by an unauthorized person. § 18.2-186.6(D).
Timing of Notification	Notice, without unreasonable delay, to any affected resident of Virginia. § 18.2-186.6(B). Notice may be reasonably delayed to allow the individual or entity to determine the scope of the breach and restore the reasonable integrity of the system. § 18.2-186.6(B). **Medical Information-Specific Statute** Notice, without unreasonable delay, to the subject of the medical information, and any affected resident of the Commonwealth. Other timing provisions apply. § 32.1-127.1:05(B).
Private Cause of Action / Enforcement / Penalties	**Enforcement:** A violation of this section by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator. § 18.2-186.6(J). A violation of this section by an individual or entity regulated by the State Corporation Commission's Bureau of Insurance shall be enforced exclusively by the State Corporation Commission. § 18.2-186.6(K). **Attorney General Enforcement: T**he Attorney General may bring an action to address violation. The Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation. This does not limit an individual from recovering direct economic damages from a violation. § 18.2-186.6(I). **Medical Information-Specific Statute** No private right of action. The statute does not explicitly provide for regulatory enforcement.
Exceptions	**Own Notification Policy:** An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information that are consistent with the timing requirements of this section, are in compliance with the notification requirements of this section if it notifies Virginia residents in accordance with its procedures in the event of a breach. § 18.2-186.6(F). **Compliance with Other Laws:**

	• **Gramm-Leach-Bliley Act:** An entity that is subject to Title V of the Gramm-Leach-Bliley Act and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section. § 18.2-186.6(G). • **Primary Regulator:** An entity that 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 shall be in compliance with this section. § 18.2-186.6(H). • **HIPAA-Covered Entities:** The notification requirements for incidents involving medical information do not apply to (i) a "covered entity" or "business associate" subject to requirements for notification in the case of a breach of protected health information (42 U.S.C. § 17932 *et seq*.) or (ii) a person or entity who is a non–HIPAA-covered entity subject to the Health Breach Notification Rule promulgated by the Federal Trade Commission pursuant to 42 U.S.C. § 17937 *et seq*.
Other Key Provisions	**Delay for Law Enforcement:** Notice required by this section may be delayed if law enforcement is notified determines and advises the entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after law enforcement determines that the notification will no longer impede the investigation or jeopardize national or homeland security. § 18.2-186.6(B).

State/Territory	**VIRGIN ISLANDS**
Statute	V.I. Code tit. 14, §§ 2208, 2209.
Definition of "Personal Information"	"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (i) Social Security number; (ii) driver's license number; or (iii) 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. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or territorial government records. § 2209(e).
Definition of "Breach"	"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by any agency. § 2209(d).
Analysis of Risk of Harm	N/A
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Personal information that is encrypted is not personal information. § 2209(e).
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. § 2209(d).
Notification Obligation	Any agency operating in the Virgin Islands that owns or licenses computerized 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 the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided below, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. § 2209(a). The notification can be made by any of the following methods: • written notice; • electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the E-SIGN Act; or • substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $100,000, or that the affected class of subject persons to be notified exceeds 50,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of (i) email notice when the person or business has an email address for the subject persons; (ii) conspicuous posting of the notice on the person or business's website page, if the person or business maintains one; and (iii) notification to major territory-wide media. § 2209(g).
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	N/A

Notification for Third-Party Data	Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. § 2209(b).
Timing of Notification	The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided below, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. § 2209(a). The notification may be delayed, if a law enforcement agency determines that the notification will impede a criminal investigation. The notification shall be made after the law enforcement agency determines that it will not compromise the investigation. § 2209(c).
Private Cause of Action / Enforcement / Penalties	N/A
Exceptions	Any agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system. § 2209(h). The notification may be delayed, if a law enforcement agency determines that the notification will impede a criminal investigation. The notification shall be made after the law enforcement agency determines that it will not compromise the investigation. § 2209(c).
Other Key Provisions	N/A

State/Territory	**WASHINGTON**
Statute	Wash. Rev. Code. §§ 19.255.005, 19.255.040 *et seq*., § 42.56.590.
Definition of “Personal Information”	Personal Information may be any of the following: (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements: (a) Social Security number; (b) Driver's license number or Washington identification card number; (c) 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, or any other numbers or information that can be used to access a person’s financial account; (d) full date of birth; (e) private key that is unique to an individual and that is used to authenticate or sign an electronic record; (f) student, military, or passport identification number; (g) health insurance policy number or health insurance identification number; (h) 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; or (i) biometric data generated by automatic measurements of an individual’s biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristic that is used to identify a specific individual. (2) Username or email address in combination with a password or security questions and answers that would permit access to an online account. (3) Any of the data elements or any combination of the date elements in (1), without the consumers first and last name, if: encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and the data element or combination of data elements would enable a person to commit identity theft against the consumer. "Personal information" does not include information that is lawfully obtained from publicly available information, of from federal, state, or local government records lawfully made available to the general public.. § 19.255.005(2).
Definition of “Breach”	Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. § 19.255.005(1).
Analysis of Risk of Harm	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. § 19.255.010(1).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	The statute does not apply to any of the elements included in the definition of “personal information” if encryption, redaction, or other methods have rendered the data element or combination of data elements unusable, and the encryption key was not accessed or acquired. § 19.255.005(2).
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure. § 19.255.005(1).
Notification Obligation	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 personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. 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. § 19.255.010(1). "Secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person. § 19.255.005(3). Notice may be provided by one of the following methods: (a) written notice; (b) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or (c) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred and fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice when the person or business has an email address for the subject persons; (ii) conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and (iii) notification to major statewide media. § 19.255.010(4). The notification must be in plain language and must include, at minimum, the following information: the name and contact information of the reporting person or business subject to the breach; a list of the types of personal information that were or are reasonably believed to have been subject to the breach; the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information; a time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and the toll-free telephone numbers and addresses of the major credit reporting agencies. § 19.255.010(6). Effective March 1, 2020, if the breach of the security of the system involves personal information including a user name or password, notice may be provided electronically or by email. However, if the breach involves login credentials of an email account furnished by the person or business, the person or business may not provide the notification to that email address, but must provide notice using another method. The notice must inform the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security questions or answer. § 19.255.010(4)(d)(i).
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	Any person or business that is required to issue a notification to more than 500 Washington residents as a result of a single breach shall notify the attorney general of the breach no more than 30 days after the breach was discovered. The notice shall include: (i) the number of Washington consumers affected by the breach, or an estimate if the exact number is not known; a list of the types of personal information that were or are reasonably believed to have been the subject of a breach; a tim eframe of exposure, if known, including the date of the breach and the time of the discovery of the breach; and a summary of steps taken to contain the breach. The notice to the Washington Attorney General must be updated if any of the required information is unknown at the time the notice is due. § 19.255.010(7).

Notification for Third-Party Data	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. § 19.255.010(2).
Timing of Notification	Notification to affected consumers under this section must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered. § 19.255.010(8).
Private Cause of Action / Enforcement / Penalties	Private Right of Action: Any consumer injured by a violation of this section may institute a civil action to recover damages. § 19.255.040(3)(a). Attorney General Enforcement: The Washington Attorney General may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this chapter. For actions brought by the Washington Attorney General to enforce the statute, the practices covered by this statute are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of the statute is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purposes of applying the consumer protection act. § 19.255.040(2).
Exceptions	Own Notification Policy: A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system. § 19.255.010(5). Delayed Notification: The notification required by this section 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. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation. § 19.255.010(3). HIPAA Covered Entity: A covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d *et seq.*, is deemed to have complied with the requirements of this section with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015. Covered entities shall notify the Washington Attorney General in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015. § 19.255.030(1). Certain Financial Institutions: A financial institution 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 is deemed to have complied with the requirements of this section with respect to "sensitive customer information" as defined in the interagency guidelines establishing information security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they existed on July 24, 2015, if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall notify the Washington Attorney General in addition to providing notice to its primary federal regulator. § 19.255.030(2).
Other Key Provisions	Waiver: Any waiver of the statute is contrary to public policy, and is void and unenforceable. § 19.255.040(1).

State/Territory	**WEST VIRGINIA**
Statute	W. Va. Code § 46A-2A-101, *et seq.*
Definition of “Personal Information”	The first name or first initial and last name linked to any one of more of the following data elements that relate to a resident of West Virginia, when the data elements are neither encrypted nor redacted: (1) Social Security number; (2) Driver’s license number or state identification card number issued in lieu of a driver’s license; or (3) Financial 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 West Virginia resident’s financial accounts. § 46A-2A-101(6). The term 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. §46A-2A-101(6).
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 regarding multiple individuals personal information and causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or fraud to any resident of West Virginia. § 46A-2A-101(1).
Analysis of Risk of Harm	If an individual reasonably believes that an unauthorized person accessed an individuals unencrypted and unredacted personal information and has caused or will cause identity theft or other fraud to any West Virginia resident, notification is required. § 46A-2A-102(a).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Notice is not required if the information is acquired in an encrypted or redacted form. However, notice is required if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that the breach has caused or will cause identity theft or other fraud to any resident of West Virginia. § 46A-2A-102(b).
Unauthorized Employee Disclosure	Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure. § 46A-2A-101(1).
Notification Obligation	An individual or entity that owns or licenses computerized data that includes personal information must give notice of any breach following discovery or notification of the breach to any resident of West Virginia whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed or acquired by an unauthorized person. § 46A-2A-102(a). Notice means: (A) written notice to the postal address in the records of the individual or entity; (B) telephonic notice; (C) Electronic notice, if consistent with 15 U.S.C. § 7001; or (D) substitute notice, if the individual or the entity demonstrates that the cost exceeds $50,000 or that the affected class of residents exceeds 100,000 persons or that the individual or entity does not have sufficient contact information or to provide notice as follows: (i) email notice; (ii) conspicuous posting of the notice on the website of the individual or the entity, if one is maintained; or (iii) notice to major statewide media. § 46A-2A-101(7).

Notification to Consumer Reporting Agencies	If more than 1,000 West Virginia residents are to be notified of a breach, the notifying entity must (without unreasonable delay) notify all consumer reporting agencies that compile and maintain files on a nationwide basis. This does not apply to an entity subject to Title V of the Gramm Leach Bliley Act, 15 U.S.C. §§ 6801, *et seq.*
Notification to Regulators	N/A
Notification for Third-Party Data	If an individual or entity maintains computerized data that includes personal information that the individual or entity does not own or license, they must give notice to the owner or licensee of the information relating to any breach of the security system as soon as practicable following the discovery of a breach. § 46A-2A-102(c).
Timing of Notification	Notice must be given without unreasonable delay except when taking measures in order to determine the scope of the breach and to restore the reasonable integrity of the system. § 46A-2A-102(a). Notification may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. After the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security, notice must be made without unreasonable delay. § 46A-2A-102(e).
Private Cause of Action / Enforcement / Penalties	If an individual fails to comply with the notice provisions of this article, it constitutes an unfair or deceptive act of practice, which can be enforced by the Attorney General. § 46A-2A-104(a). The Attorney General has exclusive authority to bring action. Civil penalties may not be assessed unless the court finds that the individual has engaged in repeated and willful violations of this article. The civil penalty cannot exceed $150,000 per breach of security of the system or series of breaches of a similar nature discovered in a single investigation. § 46A-2A-104(b). If this article is violated by a licensed financial institution, it is enforceable by the financial institution's primary functional regulator. § 46A-2A-104(c).
Exceptions	<u>Own Notification Procedures</u>: An entity that maintains its own notification procedures as part of an information privacy or security policy and are consistent with the timing requirements of this article are deemed to be in compliance with the notification requirements of this article if West Virginia residents are notified of a breach in accordance with the proper procedures. § 46A-2A-103(a). Financial Institutions: A financial institution that follows the notification guidelines 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 this article. § 46A-2A-103(b). Other: An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional regulator are deemed to be in compliance with this article. § 46A-2A-103(c).
Other Key Provisions	This article shall apply to the discovery or notification of a breach of the security of the system that occurs on or after the effective date of this article. § 46A-2A-105.

State/Territory	**WISCONSIN**
Statute	Wis. Stat. § 134.98 (2015).
Definition of “Personal Information”	An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: (1) the individual's social security number; (2) the individual's driver's license number or state identification number; (3) the number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (4) the individual's deoxyribonucleic acid profile; or (5) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation. § 134.98(1)(b).
Definition of “Breach”	There is no explicit definition of “breach.”
Analysis of Risk of Harm	Notice is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information. § 134.98(2)(cm)(1).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	Does not apply to information that is encrypted, redacted or altered in a manner that renders it unreadable. § 134.98(1)(b).
Unauthorized Employee Disclosure	An entity is not required to provide notice of the acquisition of personal information if any of the following applies: **1.** The acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information. **2.** The personal information was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity. 134.98(2)
Notification Obligation	(1) If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows 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, the entity shall make reasonable efforts to notify each subject of the personal information. § 134.98(2)(a). (2) If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. § 134.98(2)(b).

	Notice can be provided by mail or by a method the entity has previously used to communicate with the affected person. If address is not known and covered entity has not previously communicated with the affected person, covered entity must provide notice by a method reasonably calculated to actually notify the affected person. § 134.98(3)(b).
Notification to Consumer Reporting Agencies	If, as the result of a single incident, an entity is required to notify 1,000 or more individuals that PI pertaining to the individuals has been acquired, the entity shall without unreasonable delay notify all CRAs that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices sent to the individuals. § 134.98(2)(br).
Notification to Regulators	N/A
Notification for Third-Party Data	If a person, other than an individual, that stores personal information pertaining to a resident of this state, 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. § 134.98(2)(bm).
Timing of Notification	An entity shall provide the notice within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity. § 134.98(3)(a).
Private Cause of Action / Enforcement / Penalties	Civil Penalties: Failure to comply is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty. § 134.98(4).
Exceptions	Delay for Law Enforcement: A law enforcement agency may, to protect an investigation or homeland security, ask an entity not to provide a required notice for any period of time. If an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of PI, except as authorized by the law enforcement agency that made the request. § 134.98(5). Gramm-Leach-Bliley Act: An entity that is subject to, and in compliance with, the privacy and security requirements of Title V of the Gramm-Leach-Bliley Act, or a person that has a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security. § 134.98(3m)(a). HIPAA-Covered Entities: A health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form, if the entity complies with the requirements of 45 C.F.R. pt. 164. § 134.98(3m)(b).
Other Key Provisions	N/A

State/Territory	**WYOMING**
Statute	Wyo. Stat. §§ 40-12-501, *et seq.*
Definition of “Personal Information”	First name or first initial and last name of a person in combination with one or more of the following data elements, when the data elements are not redacted: (1) Social Security number; (2) driver’s license number; (3) account number, credit card number, or debit card number in combination with any security code, access code, or password that would allow access to a financial account of the person; (4) tribal ID; (5) federal or state government-issued ID; (6) shared secrets or security tokens that are known to be used for data-based authentication; (7) username or email address, in combination with a password or security question and answer that would permit access to an online account; (8) birth or marriage certificate; (9) medical information, meaning a person’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (10) health insurance information; (11) unique biometric data; (12) Individual Taxpayer Identification Number. § 40-12-501(a)(vii).
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 and causes or is reasonably believed to cause loss or injury to a resident of Wyoming. Good faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal identifying information is not used or subject to further unauthorized disclosure. § 40-12-501(a)(i).
Analysis of Risk of Harm	An individual or commercial entity must determine the likelihood that personal identifying information has been or will be misused. § 40-12-502(a).
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?	This statute only provides protection for information that is redacted. § 40-12-501(a)(vii).
Unauthorized Employee Disclosure	Good faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal identifying information is not used or subject to further unauthorized disclosure. § 40-12-501(a)(i).
Notification Obligation	When an individual or business entity that conducts business in Wyoming and that owns or licenses computerized data becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. Notice shall be made in the most expedient time possible and without unreasonable delay, 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. § 40-12-502(a). Notice to consumers may be provided by one (1) of the following methods: (i) Written notice; (ii) Electronic mail notice; (iii) Substitute notice, if the person demonstrates: (A) That the cost of providing notice would exceed ten thousand dollars ($10,000.00) for Wyoming-based persons or businesses, and two hundred fifty thousand dollars ($250,000.00) for all other businesses operating but not based in Wyoming; (B) That the affected class of subject persons to be notified exceeds ten thousand (10,000) for Wyoming-based persons or businesses and five hundred thousand (500,000) for all other businesses operating but not based in Wyoming; or (C) The person does not have sufficient contact information. § 40-12-502(d).

	Substitute notice shall consist of: (A) conspicuous posting on the Internet; and (B) notification to major statewide media, including a toll-free phone number where an individual can learn whether his or her data is included in the breach. § 40-12-502(d)(iv).
Notification to Consumer Reporting Agencies	N/A
Notification to Regulators	N/A
Notification for Third-Party Data	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. § 40-12-502(g).
Timing of Notification	Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. § 40-12-502(a).
Private Cause of Action / Enforcement / Penalties	The attorney general may bring an action in law or equity to address any violation and for other relief that may be appropriate to ensure proper compliance with this section, to recover damages, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law. § 40-12-502(f).
Exceptions	A covered entity or business associate that is subject to and complies with the Health Insurance Portability and Accountability Act, and the regulations promulgated under that act, 45 C.F.R. Parts 160 and 164, is deemed to be in compliance with this section if the covered entity or business associate notifies affected Wyoming customers or entities in compliance with the requirements of the Health Insurance Portability and Accountability Act and 45 C.F.R. Parts 160 and 164. § 40-12-502(h).
Other Key Provisions	Delay for Law Enforcement: The notification required by this section may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation. § 40-12-502(b).