State Data Breach Notification Laws

Prepared by Foley's Cybersecurity Team

FOLEY

FOLEY & LARDNER LLP

FOLEY & LARDNER LLP

State Data Breach Notification Laws

This chart should be used for informational purposes only because the recommended actions an entity should take if it experiences a security event, incident, or breach vary depending on the specific facts and circumstances. Further, data breach notification laws change frequently. The chart is a summary of basic state notification requirements that apply to entities who "own" data. This chart does not cover non-owners of data. If you do not own the data at issue, consult the applicable laws and contact legal counsel.

This chart also does not cover:

- Exceptions based on compliance with other laws, such as the Health Insurance Portability and Accountability Act (HIPAA) or Gramm-Leach-Bliley Act (GLBA).
- Exceptions regarding good faith acquisition of personally identifiable information (PII) by an employee or agent of an entity for a legitimate purpose of the entity, provided there is no further unauthorized use or disclosure of the PII.
- Exceptions regarding what constitutes PII, such as public, encrypted, redacted, unreadable, or unusable data. The chart indicates whether a safe harbor may be available for data that is considered public, encrypted, redacted, unreadable, or unusable, but the specific guidance will vary based on the circumstances. For example, some states have a safe harbor only for data that is encrypted, whereas other states may have a safe harbor for data that is encrypted or public.
- The manner in which an entity provides actual or substitute notification (e.g., via email, U.S. Mail, etc.).
- Requirements for the content of the notice.
- Any guidance materials issued by federal and state agencies.
- A comprehensive assessment of all laws applicable to breaches of information other than PII.

Current as of September 1, 2020

This chart is updated quarterly. To ensure you always refer to the most up-to-date version, please access the chart online at www.foley.com/state-data-breach-notification-laws.

For more information about state data breach notification laws or other data privacy or cybersecurity matters, please contact your Foley attorney or the following:

CHART AUTHORS

Jennifer Rathburn
Partner
Milwaukee
414.297.5864
jrathburn@foley.com

Jennifer Hennessy
Senior Counsel
Madison
608.250.7420
jhennessy@foley.com

Samuel Goldstick
Associate
Chicago
312.832.4915
sgoldstick@foley.com

ADDITIONAL CYBERSECURITY TEAM MEMBERS

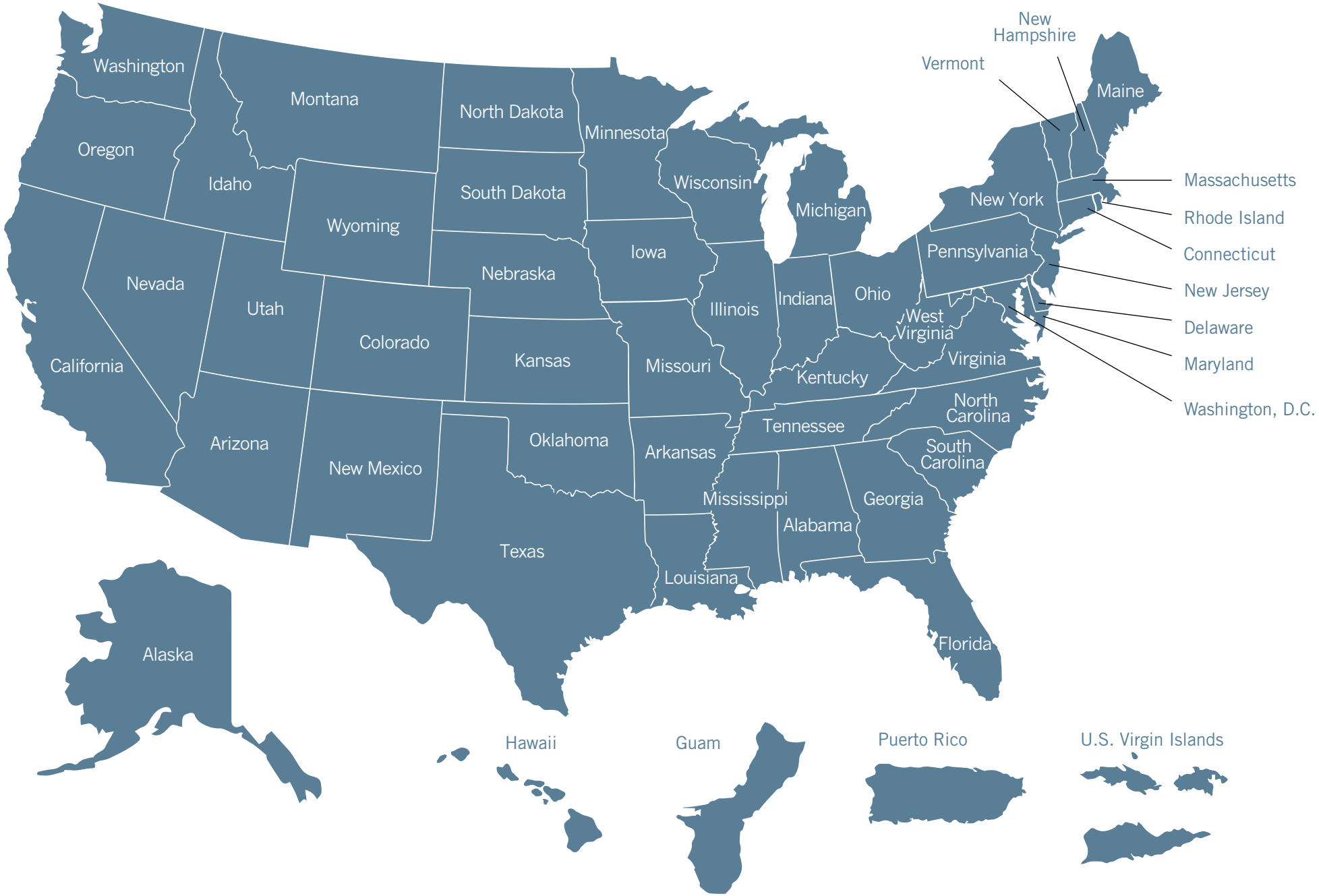
Chanley Howell
Partner
Jacksonville
904.359.8745
chowell@foley.com

Aaron Tantleff
Partner
Chicago
312.832.4367
atantleff@foley.com

Steven Millendorf
Senior Counsel
San Diego
858.847.6737
smillendorf@foley.com

FOLEY

FOLEY & LARDNER LLP



State of Residence	Alabama
Statute	Ala. Code § 8-38-1 *et seq.*
Definition of "Personal Information"	An Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident: (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. The term does not include either of the following: (1) information about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media; or (2) 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.
Definition of "Breach"	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 any of 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; or (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. In determining whether sensitive personally identifying information has been acquired, or is reasonably believed to have been acquired, by an unauthorized 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, such as a lost or stolen computer or other device containing information; (2) indications that the information has been downloaded or copied; (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or (4) whether the information has been made public.
Analysis of Risk of Harm	Notification is not required if, after a good faith and prompt investigation, it is determined that the breach is not reasonably likely to cause substantial harm to the individuals to whom the information relates.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.

[1] *See also* "Definition of 'Personal Information'" and "Definition of 'Breach'" columns.

State of Residence	Alabama continued
Timing of Notification to Individuals	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. Absent a law enforcement delay permitted under this statute, 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. If a federal or state law enforcement agency determines that the required notice to individuals 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. A law enforcement agency, by a subsequent written request, may revoke the delay as of a specified date or extend the period set forth in the original request made under this section if further delay is necessary.
Notifications to Regulators[2]	If the number of individuals a covered entity is required to notify exceeds 1,000 individuals, the entity shall provide written notice of the breach to the Attorney General as expeditiously as possible and without unreasonable delay. Absent a delay by law enforcement permitted under this statute, the covered entity shall provide the 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 entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates. If a covered entity discovers circumstances requiring notice 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. § 1681a, of the timing, distribution, and content of the notices.
Enforcement/Private Cause of Action/ Penalties[3]	A violation of the notification provisions is considered an unlawful trade practice under the Alabama Deceptive Trade Practices Act ("ADTPA"), but does not constitute a criminal offense. There is no private right of action. However, the Office of the Attorney General may enforce violations of the Alabama Data Breach Notification Act as a deceptive trade practice and maintains exclusive authority to bring an action for civil penalties. Any covered entity or third party agent that knowingly (i.e., willfully or with reckless disregard) violates the notification requirements could be subject to penalties of up to $500,000 per breach under the ADTPA. In addition to these penalties, a covered entity violating the breach notification provisions shall be liable for a penalty of up to $5,000 per day for each consecutive day it fails to take reasonable action to comply with the notice provisions. The Attorney General also has authority to bring an action for damages in a representative capacity on behalf of any named individuals. In such an action, recovery is limited to actual damages suffered by those individuals, plus reasonable attorneys' fees and costs.

[2] *See also* "Analysis of Risk of Harm" column.

[3] There may be other applicable penalties and enforcement actions depending on the facts and circumstances.

State of Residence	Alaska
Statute	Alaska Stat. § 45.48.010 *et seq.*
Definition of "Personal Information"	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; in this subparagraph, "individual's name" means a combination of an individual's (1) first name or first initial; and (2) last name; and (B) One or more of the following information elements: (1) the individual's Social Security number; (2) the individual's driver's license number or state identification card number; (3) the individual's account number, credit card number, or debit card number; (4) if an account can only be accessed with a personal code, the individual's account number, credit card number, or debit card number and the personal code; (5) passwords, personal identification numbers, or other access codes for financial accounts. "Personal code" means a security code, an access code, a personal identification number, or a password.
Definition of "Breach"	Unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector. Acquisition includes acquisition by: (1) photocopying, facsimile, or other paper-based method; (2) a device, including a computer, that can read, write, or store information that is represented in numerical form; or (3) a method not identified above.
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.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	An information collector shall make the disclosure required in the most expeditious time possible and without unreasonable delay, except as provided below and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system. An information collector may delay disclosing the breach 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.
Notifications to Regulators[2]	If an information collector is required 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.

State of Residence	Alaska continued
Enforcement/Private Cause of Action/ Penalties[3]	The violation is an unfair or deceptive act or practice. Civil penalty payable to state of up to $500 for each state resident who was not notified, except that the total civil penalty may not exceed $50,000. Penalties for private actions are limited to actual economic damages. 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, 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.

State of Residence	Arizona
Statute	Ariz. Rev. Stat. § 18-551 *et seq.*
Definition of "Personal Information"	"Personal Information" means any of the following: (A) An individual's first name or first initial and last name in combination with any one or more of the following specified data elements: (1) an individual's Social Security number; (2) the number on an individual's driver license issued pursuant to § 28-3166 or non-operating identification license issued pursuant to § 28-3165; (3) a private key that is unique to an individual and that is used to authenticate or sign an electronic record; (4) an individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would allow access to the individual's financial account; (5) an individual's health insurance identification number; (6) information about an individual's medical or mental health treatment or diagnosis by a health care professional; (7) an individual's passport number; (8) an individual's taxpayer identification number or an identity protection personal identification number issued by the IRS; or (9) unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account. (B) An individual's username or email address, in combination with a password or security question and answer, that allows access to an online account.
Definition of "Breach"	An unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information maintained as part of a database of personal information regarding multiple individuals.
Analysis of Risk of Harm	If a person that conducts business in Arizona and that owns, maintains or licenses unencrypted and unredacted 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 "security incident" is 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 systems or data may have failed. A person is not required to provide notice of a security system breach if that person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Notice shall be made within 45 days after a determination that a breach has occurred. The notification may be delayed if a law enforcement agency advises the person that the notification will impede a criminal investigation. Upon being informed that the notifications no longer compromise the investigation, the person shall make the required notifications, as applicable, within 45 days.
Notifications to Regulators[2]	If the breach requires notification to more than 1,000 individuals, notice also must be provided to the three largest nationwide consumer reporting agencies and to the Arizona Attorney General in writing, along with a copy of the notice sent to affected individuals.
Enforcement/Private Cause of Action/ Penalties[3]	The Arizona Attorney General retains exclusive authority to enforce willful and knowing violations of this statute, and may seek a civil penalty "not to exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals," with a "maximum civil penalty from a breach or series of related breaches" of $500,000. The Attorney General is entitled to recover restitution for affected individuals.

State of Residence	Arkansas
Statute	Ark. Code § 4-110-101 *et seq.*
Definition of "Personal Information"	An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements when either the name or the data element is not encrypted or redacted: (1) Social Security number; (2) driver's license number or Arkansas identification card number; (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; (3) medical information; or (4) biometric data.
Definition of "Breach"	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.
Analysis of Risk of Harm	Notification is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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 or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required shall be made after the law enforcement agency determines that it will not compromise the investigation.
Notifications to Regulators[2]	If a breach affects 1,000 or more individuals, the person or business required to make a disclosure of the breach under this law shall, at the same time the 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 breach to the Arkansas Attorney General.
Enforcement/Private Cause of Action/ Penalties[3]	Any violation of this chapter is punishable by action of the attorney general under the provisions of § 4-88-101 *et seq.* (deceptive trade practice).

State of Residence	California
Statute	Cal. Civ. Code § 1798.80 *et seq.*; Cal. Health & Safety Code § 1280.15
Definition of "Personal Information"	(A) An individual's first name or first initial and his or her 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 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; (3) 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; (4) medical information; (5) health insurance information; (6) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes; (7) information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5. (B) A username or email address in combination with a password or security question and answer that would permit access to an online account. **Medical Information-Specific Statute** For clinics, health facilities, home health agencies, and hospices licensed pursuant to sections 1204, 1250, 1725, or 1745 of the Cal. Health & Safety Code, the Medical Information Breach Notification statute may apply. The statute applies to patients' medical information. "Medical information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.
Definition of "Breach"	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. **Medical Information-Specific Statute** Unlawful or unauthorized access to or use or disclosure of a patient's medical information, whether in paper or electronic form, triggers the notification requirement.
Analysis of Risk of Harm	NONE
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances. **Medical Information-Specific Statute** There is not an explicit exception for information that is encrypted, redacted, or made unreadable.
Timing of Notification to Individuals	The disclosure 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. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation. **Medical Information-Specific Statute** The covered entity must notify affected persons no later than 15 business days after the unauthorized access, use, or disclosure has been detected. The covered entity may delay notice for law enforcement purposes under certain circumstances.

State of Residence	California continued
Notifications to Regulators[2]	A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the attorney general. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code. **Medical Information-Specific Statute** A covered entity must notify the California Department of Health Services no later than 15 days after it detects the unauthorized access, use, or disclosure.
Enforcement/Private Cause of Action/ Penalties[3]	Any customer injured by a violation of this title may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined. **Medical Information-Specific Statute** No private right of actions for violations. The California Department of Health Services may impose the following penalties against covered entities that violate the medical information statute: (1) $25,000 per patient whose information was unlawfully or without authorization accessed, used, or disclosed; (2) up to $17,500 per subsequent occurrence of unlawful or unauthorized access, use, or disclosure of that patient's medical information; and/or (3) if the entity fails to provide timely notice, $100 per day after the first 15 day period. Total penalties for a single event may not exceed $250,000.

State of Residence	Colorado
Statute	Colo. Rev. Stat. § 6-1-716
Definition of "Personal Information"	"Personal Information" means any of the following: (A) 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: (1) Social Security number; (2) student, military, or passport identification number; (3) driver's license number or identification card number; (4) medical information; (5) health insurance identification number; or (6) biometric data; or (B) 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) 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.
Definition of "Breach"	Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.
Analysis of Risk of Harm	A covered entity that maintains, owns, or licenses computerized personal information shall, when it becomes aware that a security breach may have occurred, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The covered entity shall give notice to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. 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.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Notice must be made in the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determining that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. "Determination that a security breach occurred" means the point in time in which there is sufficient evidence to conclude that a security breach has taken place. 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 for providing individual notice controls. Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the covered entity that conducts business in Colorado not to send notice required by this section. Notice must be made in good faith, in the most expedient time possible and without unreasonable delay and as soon as possible but not later than 30 days after the law enforcement agency determines that notification will no longer impede the investigation and has notified the covered entity that conducts business in Colorado that it is appropriate to send the notice required by this section.

State of Residence	Colorado continued
Notifications to Regulators[2]	If a covered entity is required to notify more than 500 Colorado residents of any security breach, the covered entity must also provide notice of the breach to the Colorado Attorney General in the most expedient time possible and without unreasonable delay, but not later than 30 days after the data of determination that a security breach occurred. If a covered entity is required to notify more than 1,000 Colorado residents of a security breach, the covered entity must 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. § 1681a(p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. Nothing in this section shall be construed to require the individual or commercial entity to provide to the consumer reporting agency the names or other personal information of breach notice recipients.
Enforcement/Private Cause of Action/ Penalties[3]	The Colorado Attorney General may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. These provisions are not exclusive and do not relieve a person or entity subject to this section from compliance with all other applicable provisions of law.

State of Residence	Connecticut
Statute	Conn. Gen. Stat. § 36a-701b
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: (1) Social Security number; (2) driver's license number or state identification card number; or (3) 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.
Definition of "Breach"	Unauthorized access to or unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.
Analysis of Risk of Harm	Notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Notice shall be made without unreasonable delay but not later than ninety days after the discovery of such breach, unless a shorter time is required under federal law, subject to delay by law enforcement and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system. Any notification shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.
Notifications to Regulators[2]	The person 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.
Enforcement/Private Cause of Action/ Penalties[3]	If residents' Social Security numbers are compromised, or reasonably believed to have been compromised, as the result of a breach, the breached entity must offer identity theft protection services at no cost to those residents for at least 24 months. Failure to comply with the requirements of this section shall constitute an unfair trade practice for the purposes of section 42-110b and shall be enforced by the attorney general.

State of Residence	Delaware
Statute	Del. Code Ann. tit. 6 § 12B-101 *et seq.*
Definition of "Personal Information"	A Delaware resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident: (1) Social Security number; (2) driver's license number or state or federal 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) 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 healthcare 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; and (9) an individual taxpayer identification number.
Definition of "Breach"	The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. 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 who owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.
Analysis of Risk of Harm	Any person who conducts business in Delaware and who owns or licenses computerized data that includes personal information shall provide notice of any breach of security following determination of the breach of security to any resident of Delaware whose personal information was breached or is reasonably believed to have been breached, unless, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Notice must be made without unreasonable delay but not later than 60 days after determination of a security breach. "Determination of the breach of security" means the point in time at which a person who owns, licenses, or maintains computerized data has sufficient evidence to conclude that a breach of security of such computerized data has taken place. Notice may be delayed if the person could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of Delaware was included in a breach of security, and in such case notice must be provided as soon as practicable after the determination that the breach of security included the personal information of such residents, unless such person provides or has provided substitute notice in accordance with this chapter. Notice may also be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and has made a request of the person that the notice be delayed. Any such delayed notice must be made after the law enforcement agency determines that notice will not compromise the criminal investigation and notifies the person of such determination.
Notifications to Regulators[2]	If the affected number of Delaware residents to be notified exceeds 500 residents, the person required to provide notice shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Delaware Attorney General.

State of Residence	Delaware continued
Enforcement/Private Cause of Action/ Penalties[3]	Pursuant to the enforcement duties and powers of the Director of Consumer Protection of the Department of Justice, 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 this chapter are not exclusive and do not relieve an individual or a commercial entity subject to this chapter from compliance with all other applicable provisions of law. If the breach involves Social Security numbers, the breached entity is required to provide credit monitoring services for at least one (1) year to any residents whose Social Security numbers were compromised, or reasonably believed to have been compromise, as the result of a breach. However, if the entity conducts an appropriate investigation and reasonably determines that the breach is unlikely to result in harm to the individuals whose personal information was breached, the entity does not need to provide credit monitoring services.

State of Residence	District of Columbia
Statute	D.C. Code § 28-3851 *et seq.*
Definition of "Personal Information"	"Personal information" means: (A) 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; (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, first initial and last name, or other independent personal identifier; or (B) A username or email address in combination with a password, security question and answer, or other means of authentication, or any combination of data elements included in sub-sub-subparagraphs (1) through (6) of the above sub-subparagraph that permits access to an individual's email account.
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 entity who conducts business in the District of Columbia.
Analysis of Risk of Harm	The term "breach of the security of the system" does not include acquisition of personal information of an individual that the person or entity reasonably determines, after a reasonable investigation and consultation with the Office of the Attorney General for the District of Columbia and federal law enforcement agencies, will likely not result in harm to the individual.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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. The notification required by this section 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.

State of Residence	District of Columbia continued
Notifications to Regulators[2]	If the breach affects 50 or more residents of the District of Columbia, the person or entity required to give notice to those individuals shall promptly also provide written notice of the breach of the security of the system to the Office of the Attorney General for the District of Columbia. This notice shall be made in the most expedient manner possible, without unreasonable delay, and in no event later than when notice is provided to residents of the District of Columbia. Such notification shall not be delayed on the grounds that the total number of District residents affected by the breach has not yet been ascertained. Notification to the Office of the Attorney General for the District of Columbia 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. If any person or entity is required to notify more than 1,000 persons of a breach of security, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act, approved October 26, 1970 (84 Stat. 1128; 15 U.S.C. § 1681a(p)), of the timing, distribution, and content of the notices. Nothing in this subsection shall be construed to require the person to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.
Enforcement/Private Cause of Action/ Penalties[3]	A violation of this subchapter, or any rule issued pursuant to the authority of this subchapter, is an unfair or deceptive trade practice pursuant to § 28-3904(kk). The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law. When a person or entity experiences a breach of the security of the system that requires notification, 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 Taxpayer 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 under this section.

State of Residence	Florida
Statute	Fla. Stat. § 501.171
Definition of "Personal Information"	(A) 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 (B) 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.
Definition of "Breach"	Unauthorized access of data in electronic form containing personal information.
Analysis of Risk of Harm	Notice is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered 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 five years. The covered entity shall provide the written determination to the Department of Legal Affairs within 30 days after the determination.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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 individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay. May receive 15 additional days if good cause is provided in writing to the Department of Legal Affairs within 30 days after determination of the breach or reason to believe the breach occurred. 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 that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified date if further delay is necessary.

State of Residence	Florida continued
Notifications to Regulators[2]	Notice to Department of Legal Affairs required for notification to more than 500 individuals. Must be provided as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred. 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. A covered entity may provide the Department of Legal Affairs with supplemental information regarding a breach at any time. If a covered entity discovers circumstances requiring notice of more than 1,000 individuals at a single time, the covered 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. § 1681a(p), of the timing, distribution, and content of the notices.
Enforcement/Private Cause of Action/ Penalties[3]	A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the department under s. 501.207 against a covered entity or third-party agent. 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 in this paragraph apply per breach and not per individual affected by the breach. All penalties collected pursuant to this subsection shall be deposited into the General Revenue Fund. This section does not establish a private cause of action.

State of Residence	Georgia
Statute	Ga. Code § 10-1-910 *et seq.*
Definition of "Personal Information"	(A) 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 (B) Any of the above items when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.
Definition of "Breach"	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.
Analysis of Risk of Harm	NONE
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The 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. The notification may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification shall be made after the law enforcement agency determines that it will not compromise the investigation.
Notifications to Regulators[2]	In the event that an information broker or data collector discovers circumstances requiring notification 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 U.S.C. Section 1681a, of the timing, distribution, and content of the notices.
Enforcement/Private Cause of Action/ Penalties[3]	NONE

State of Residence	Hawaii
Statute	Haw. Rev. Stat. § 487N-1 *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 either the name or the data elements are not encrypted: (1) Social Security number; (2) driver's license number or Hawaii identification card number; or (3) account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.
Definition of "Breach"	Unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information, through use of a key or otherwise, where illegal use of the personal information has occurred or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process of key constitutes a security breach. *Note: "Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.
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?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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. The notice shall be delayed if a law enforcement agency informs the entity that notification may impede a criminal investigation or jeopardize national security and requests a delay; provided that such request is made in writing, or the entity documents the 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 shall be provided without unreasonable delay after the law enforcement agency communicates to the entity its determination that notice will no longer impede the investigation or jeopardize national security.
Notifications to Regulators[2]	In the event an entity provides notice to more than 1,000 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.
Enforcement/Private Cause of Action/ Penalties[3]	Any business that violates any provision of this chapter shall be subject to penalties of not more than $2,500 for each violation. The attorney general or the executive director of the Office of Consumer Protection may bring an action pursuant to this section. In addition to any penalty provided for above, any business that violates any provision of this chapter 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 section may award reasonable attorneys' fees to the prevailing party. The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this State.

State of Residence	Idaho
Statute	Idaho Code § 28-51-104 *et seq.*
Definition of "Personal Information"	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 Idaho 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 a resident's financial account.
Definition of "Breach"	Illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons maintained by an agency, an individual or a commercial entity.
Analysis of Risk of Harm	A city, county, or state agency, or an individual or a commercial entity 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, the individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident. Also, if the definition of "breach" is not met, then notice is not required.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Notice must 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, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system. Notice may be delayed if a law enforcement agency advises the agency, the individual or the commercial entity that the notice will impede a criminal investigation. Notice must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency advises the agency, the individual or the commercial entity that notification will no longer impede the investigation.
Notifications to Regulators[2]	NONE
Enforcement/Private Cause of Action/ Penalties[3]	In any case in which an agency's, commercial entity's, or individual's primary regulator has reason to believe that an agency, an individual or a commercial entity subject to that primary regulator's jurisdiction under section 28-51-104(6), Idaho Code, has violated section 28-51-105, Idaho Code, by failing to give notice in accordance with that section, the primary regulator may bring a civil action to enforce compliance with that section and enjoin that agency, individual or commercial entity from further violations. Any agency, individual or commercial entity that intentionally fails to give notice in accordance with section 28-51-105, Idaho Code, shall be subject to a fine of not more than $25,000 per breach of the security of the system.

State of Residence	Illinois
Statute	815 Ill. Comp. Stat. 530/5 *et seq.*
Definition of "Personal Information"	"Personal Information" means either of the following: (A) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted, or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: (1) Social Security number; (2) driver's license number or State identification card number; (3) account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) medical information; (5) health insurance information; or (6) unique biometric data. (B) Username or email address, in combination with a password or security question and answer that would permit access to an online account, when either the username or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.
Definition of "Breach"	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.
Analysis of Risk of Harm	NONE
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The disclosure notification 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 restore the reasonable integrity, security, and confidentiality of the data system. The notification to an Illinois resident 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.
Notifications to Regulators[2]	Any data collector required to issue notice to more than 500 Illinois residents as a result of a single breach of the security system shall notify the Illinois Attorney General of the breach in the most expedient time possible and without unreasonable delay but in no event later than when the data collector provides notice to Illinois residents. State agencies must report security breaches involving more than 250 Illinois residents to the attorney general, including the types of personal information compromised, the number of Illinois residents affected, any steps the agency has taken or plans to take to notify consumers, and the date and timeframe of the breach, if known. Such notification must be made within 45 days of the agency's discovery of the security breach or when the agency provides notice to consumers, whichever is sooner, unless there is good cause for reasonable delay. If the date or timeframe of the breach is unknown at the time the notice is sent to the attorney general, the State agency shall send the attorney general the date or timeframe of the breach as soon as possible. If the State 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' personal information, the agency is required to notify both the Chief Information Security Officer of the Department of Innovation and Technology and the Illinois Attorney General without delay but no later than 72 hours following discovery. Any covered entity or business associate that is subject to and in compliance with HIPAA shall be deemed to be in compliance with the provisions of this Act, provided that any covered entity or business associate required to provide notification of a breach to the Secretary of Health and Human Services pursuant to HIPAA also provides such notification to the Illinois Attorney General within 5 business days of notifying the Secretary.

State of Residence	Illinois continued
Enforcement/Private Cause of Action/ Penalties[3]	A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

State of Residence	Indiana
Statute	Ind. Code § 24-4.9-1-1 *et. seq*
Definition of "Personal Information"	(A) A Social Security number that is not encrypted or redacted; or (B) An individual's first and last names, or first initial and last name, and one or more of the following data elements that are not encrypted or redacted: (1) a driver's license number; (2) a state identification card number; (3) a credit card number; or (4) a financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.
Definition of "Breach"	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an entity. The term includes the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format. The term does not include unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key: (1) has not been compromised or disclosed; and (2) is not in the possession of or known to the person who, without authorization, acquired, or has access to the portable electronic device.
Analysis of Risk of Harm	After discovering or being notified of a breach of the security of data, the data base owner shall disclose the breach to an Indiana resident whose: (1) unencrypted personal information was or may have been acquired by an unauthorized person; or (2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5- 3.5), identity theft, or fraud affecting the Indiana resident.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	A person required to make a disclosure or notification under this chapter shall make the disclosure or notification without unreasonable delay. For purposes of this section, a delay is reasonable if the delay 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 a law enforcement agency to delay disclosure because disclosure will: (a) impede a criminal or civil investigation; or (b) jeopardize national security. A person required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after: (1) delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or (2) the attorney general or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security.
Notifications to Regulators[2]	A data base owner required to make a disclosure to more than 1,000 consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system. If a data base owner makes a disclosure to individuals, the data base owner shall also disclose the breach to the attorney general.

State of Residence	Indiana continued
Enforcement/Private Cause of Action/ Penalties[3]	A person who is required to make a disclosure or notification and who fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general under this chapter. A failure to make a required disclosure or notification in connection with a related series of breaches of the security of data constitutes one deceptive act. 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; (2) a civil penalty of not more than $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.

Return to Map

State of Residence	Iowa
Statute	Iowa Code § 715C.1 *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 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) financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account; (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) unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
Definition of "Breach"	Unauthorized acquisition of personal information maintained in computerized form by a person who 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.
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.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances where 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). In order to qualify as "encrypted," the algorithmic method used must meet accepted industry standards.
Timing of Notification to Individuals	The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data. The consumer notification requirements 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. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the person required to give notice in writing.
Notifications to Regulators[2]	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 requiring notification to more than 500 residents of this state shall give written notice of the breach of security to the director of the consumer protection division of the office of the attorney general within five business days after giving notice of the breach of security to any consumer pursuant to this section.
Enforcement/Private Cause of Action/ Penalties[3]	A violation of this chapter is an unlawful practice pursuant to section 714.16 and, in addition to the remedies provided to the attorney general pursuant to section 714.16, subsection 7, 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 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.

State of Residence	Kansas
Statute	Kan. Stat. § 50-7a01 *et seq.*
Definition of "Personal Information"	A consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted: (1) Social Security number; (2) driver's license number or state identification card number; or (3) financial account number, or credit or debit card number, alone or in combination with any required security code, access code, or password that would permit access to a consumer's financial account.
Definition of "Breach"	Unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer.
Analysis of Risk of Harm	A person who 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. Also, if the definition of "breach" is not met, then notice is not required.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Notice must 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. 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.
Notifications to Regulators[2]	In the event that a person discovers circumstances requiring notification pursuant to this section of more than 1,000 consumers at one time, the person 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. § 1681a(p), of the timing, distribution, and content of the notices.
Enforcement/Private Cause of Action/ Penalties[3]	Entity other than insurance company: 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. Insurance companies: the insurance commissioner shall have the sole authority to enforce the provisions of this section.

State of Residence	Kentucky
Statute	Ky. Rev. Stat. § 365.732
Definition of "Personal Information"	An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or data element is not redacted: (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 to permit access to an individual's financial account.
Definition of "Breach"	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.
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?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The disclosure 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. The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.
Notifications to Regulators[2]	If a person discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a, of the timing, distribution, and content of the notices.
Enforcement/Private Cause of Action/ Penalties[3]	NONE

State of Residence	Louisiana
Statute	La. Rev. Stat. § 51:3071 *et seq.* La. Admin. Code tit. 16, § 701
Definition of "Personal Information"	"Personal Information" means the first name or first initial and last name of an individual resident of Louisiana in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: (1) Social Security number; (2) driver's license number or state identification card number; (3) 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; (4) passport number; or (5) biometric data.
Definition of "Breach"	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.
Analysis of Risk of Harm	Notification shall not be required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to the residents of Louisiana. The person or business shall retain a copy of the written determination and supporting documentation for five (5) years from the date of discovery of the breach of the security system. If requested in writing, the person or business shall send a copy of the written determination and supporting documentation to the attorney general no later than 30 days from the date of receipt of the request.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notification shall be made in the most expedient time possible and without unreasonable delay, but not later than 60 days from the discovery of the breach, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. If a law enforcement agency determines that the notification would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation. When notification is delayed pursuant to a law enforcement delay or due to a determination by the person or agency that measures are necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system, the person or agency shall provide the attorney general the reasons for the delay in writing within the 60-day notification period. Upon receipt of the written reasons, the attorney general shall allow a reasonable extension of time to provide the required notification.
Notifications to Regulators[2]	When notice to residents is required, the person shall provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the attorney general's office. Notice shall include the names of all residents affected by the breach. Notice is timely if received within 10 days of distribution of notice to residents.
Enforcement/Private Cause of Action/ Penalties[3]	A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information. Failure to provide timely notice to the attorney general may be punishable by a fine not to exceed $5,000 per violation. Each day notice is not received by the attorney general is a separate violation. A violation of the notification provisions is also deemed an unfair act or trade practice under R.S. 51:1405(A).

State of Residence	Maine
Statute	10 Me. Rev. Stat. § 1346 *et seq.*
Definition of "Personal Information"	(A) 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 data elements are not encrypted or redacted: (1) a Social Security number; (2) a 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; or (4) account passwords or personal identification numbers or other access codes; or (B) Any of the above data elements when not in connection with the individual's name, if the information, if compromised, would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.
Definition of "Breach"	Unauthorized acquisition, release, or use of an individual's computerized data that includes personal information that compromises the security, confidentiality, or integrity of personal information of the individual maintained by a person.
Analysis of Risk of Harm	If any person becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The 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. If, after the completion of an investigation to determine the likelihood that personal information 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.
Notifications to Regulators[2]	If a person discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the person shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a(p). Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach. When notice of a breach of the security of the system is required, the person shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the attorney general.

State of Residence	Maine continued
Enforcement/Private Cause of Action/ Penalties[3]	The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any person who is licensed or regulated by those regulators. The attorney general shall enforce this chapter for all other persons. A person 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 person 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. 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.

State of Residence	Maryland
Statute	Md. Code Com. Law § 14-3501 *et seq.*
Definition of "Personal Information"	(A) 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) a Social Security number, individual taxpayer identification number, 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 (and any other information created by an entity covered by HIPAA regarding an individual's medical history, medical condition, or medical treatment or diagnosis); (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; (6) biometric data of an individual generated by automatic measurements of an 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 (B) A username or email address in combination with a password or security question and answer that permits access to an individual's email account.
Definition of "Breach"	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business.
Analysis of Risk of Harm	A business, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused as a result of the breach. If, after the investigation is concluded, the business determines that the breach creates a likelihood that the person information has been or will be misused, the business shall notify the individual of the breach. If notice is not required, the business shall maintain records that reflect its determination for three years (3) after the determination is made.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notice shall be given as soon as reasonably practicable, but not later than 45 days after the business concludes its investigation. Notice may be delayed: (1) if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or (2) to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system. If notification is delayed by law enforcement, 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.
Notifications to Regulators[2]	Prior to giving the individual notification required under subsection and subject to law enforcement delay, a business shall provide notice of a breach of the security of a system to the office of the attorney general. If a business is required to give notice of a breach of the security of a system to 1,000 or more individuals, the business also shall notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notices. This does not require the inclusion of the names or other personal identifying information of recipients of notices of the breach of the security of a system.

State of Residence	Maryland continued
Enforcement/Private Cause of Action/ Penalties[3]	A violation: (1) Is an unfair or deceptive trade practice; and (2) Is 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.

State of Residence	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 one 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.
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 personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident. *Note: "Data" means any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.
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?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	A person or agency shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose to such resident. Notice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay. The person or agency shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided, however, that such disclosure shall not require the disclosure of confidential business information or trade secrets. Notice shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information. As a result, the person or agency must send out additional notifications on a rolling basis, as necessary.
Notifications to Regulators[2]	A person or agency shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general and the director of consumer affairs and business regulation. Upon receipt of this notice, the director shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice to the consumer reporting agencies and state agencies identified by the director. Any person who experienced a breach involving a resident's Social Security number shall also file a report with the attorney general and the director of consumer affairs and business regulation certifying that their credit monitoring services are compliant with state law.

State of Residence	Massachusetts continued
Enforcement/Private Cause of Action/ Penalties[3]	The attorney general may bring an action pursuant to section 4 of chapter 93A (unfair trade practice) against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate. If residents' Social Security numbers are disclosed, or reasonably believed to have been disclosed, as the result of a breach, the breached entity must offer credit monitoring services to those residents at no cost for at least 18 months (42 months if the entity is a consumer reporting agency). Breached entities are prohibited from asking residents to waive their right to a private action as a condition for receiving credit monitoring services.

Return to Map

State of Residence	Michigan
Statute	Mich. Comp. Laws §§ 445.63, .72
Definition of "Personal Information"	The first name or first initial and last name linked to one or more of the following data elements of a resident of this state: (1) Social Security number; (2) driver's 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.
Definition of "Breach"	Unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals.
Analysis of Risk of Harm	Unless the person or agency 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 this state, a person or agency that discovers a security breach, or receives notice of a security breach by an entity that maintains information on behalf of another entity, shall provide a notice of the security breach to each resident of this state who meets one or more of the following: (1) that resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person; (2) that resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key. In determining whether a security breach is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of this state, a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	A person or agency shall provide any notice required under this section without unreasonable delay. A person or agency may delay providing notice without violating this subsection if either of the following is met: (1) A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. However, the agency or person shall provide the notice required under this subsection without unreasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. (2) A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the agency or person shall provide the notice required under this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.
Notifications to Regulators[2]	After a person or agency provides a notice under this section, the person or agency shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the security breach without unreasonable delay. A notification shall include the number of notices that the person or agency provided to residents of this state and the timing of those notices. This does not apply if the following is met: The person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents of this state.
Enforcement/Private Cause of Action/ Penalties[3]	A person who knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice. The attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section. The aggregate liability of a person for civil fines for multiple violations that arise from the same security breach shall not exceed $750,000. This does not affect the availability of any civil remedy for a violation of state or federal law.

State of Residence	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.
Definition of "Breach"	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the business.
Analysis of Risk of Harm	NONE
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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 any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system. Notification may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.
Notifications to Regulators[2]	If a person discovers circumstances requiring notification of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.
Enforcement/Private Cause of Action/ Penalties[3]	The attorney general shall enforce this section under section 8.31 (additional duties of attorney general).

State of Residence	Mississippi
Statute	Miss. Code § 75-24-29
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's license number or state identification card number; or (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 an individual's financial account.
Definition of "Breach"	Unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.
Analysis of Risk of Harm	Notification shall not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The disclosure shall be made without unreasonable delay, subject to notification by an entity that maintains information, delay by law enforcement, and the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system. Any 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. Any such delayed notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and so notifies the person of that determination.
Notifications to Regulators[2]	NONE
Enforcement/Private Cause of Action/ Penalties[3]	Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the attorney general; however, nothing in this section may be construed to create a private right of action.

State of Residence	Missouri
Statute	Mo. Rev. Stat. § 407.1500
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 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; or (6) health insurance information.
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.
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. Such a determination shall be documented in writing and the documentation shall be maintained for five years.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The disclosure notification shall be: (1) Made without unreasonable delay (2) Consistent with the legitimate needs of law enforcement, as provided in this section (3) 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 The notice may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the person 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 shall be provided without unreasonable delay after the law enforcement agency communicates to the person its determination that notice will no longer impede the investigation or jeopardize national or homeland security.
Notifications to Regulators[2]	In the event a person provides notice to more than 1,000 consumers at one time pursuant to this section, the person shall notify, without unreasonable delay, 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. Section 1681a(p), of the timing, distribution, and content of the notice.
Enforcement/Private Cause of Action/ Penalties[3]	The attorney general shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed $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.

State of Residence	Montana
Statute	Mont. Code §§ 30-14-1701–1702, 1704
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) 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; (4) medical record information as defined in 33–19–104; (5) a taxpayer identification number; or (6) an identity protection personal identification number issued by the United States Internal Revenue Service.
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.
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?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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. 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.
Notifications to Regulators[2]	If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals. Any person or business that is required to issue a notification pursuant to this section shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the attorney general's consumer protection office, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification.
Enforcement/Private Cause of Action/ Penalties[3]	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 pursuant to 30-14-111(2). The provisions of 30-14-111(3) and (4) and 30-14-112 through 30-14-115 apply to this part. A violation of this part is a violation of 30-14-103, and the penalties for a violation of this part are as provided in 30-14-142.

State of Residence	Nebraska
Statute	Neb. Rev. Stat. § 87-801 *et seq*.
Definition of "Personal Information"	Personal information means either of the following: (A) A Nebraska 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 if either the name or 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: (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; or (B) A username or email address, in combination with a password or security question and answer, that would permit access to an online account.
Definition of "Breach"	Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.
Analysis of Risk of Harm	Notification is required if a reasonable and prompt investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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. 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.
Notifications to Regulators[2]	If notice of a breach of security of the system is required, the individual or commercial entity shall also, not later than the time when notice is provided to the Nebraska resident, provide notice of the breach of security of the system to the attorney general.
Enforcement/Private Cause of Action/ Penalties[3]	The attorney general may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of the act.

Return to Map

State of Residence	Nevada
Statute	Nev. Rev. Stat. 603A.010 *et seq.*
Definition of "Personal Information"	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: (1) Social Security number; (2) driver's license number, driver authorization card number, or ID card number; (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 the person's financial account; (4) medical identification number or health insurance ID number; or (5) username, unique identifier, or electronic mail address in combination with a password, access code, or security question and answer that would permit access to an online account.
Definition of "Breach"	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the data collector.
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?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification must be made after the law enforcement agency determines that the notification will not compromise the investigation.
Notifications to Regulators[2]	Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals at any one time.
Enforcement/Private Cause of Action/ Penalties[3]	If the attorney general or a district attorney has reason to believe that any person is violating, proposes to violate or has violated the provisions of this chapter, the attorney general or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation.

State of Residence	New Hampshire
Statute	N.H. Rev. Stat. §§ 359-C:19– C:21; N.H. Rev. Stat. § 332-I:5
Definition of "Personal Information"	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. **Medical Information-Specific Statute** For persons, corporations, facilities, or institutions either licensed in New Hampshire or otherwise lawfully providing health care services, New Hampshire has a statute that requires notification if a health care provider or its business associate improperly discloses medical information for marketing or fundraising purposes in violation of New Hampshire law.
Definition of "Breach"	Unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state.
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.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The person shall notify the affected individuals as soon as possible as required under this subdivision. 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.
Notifications to Regulators[2]	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 New Hampshire attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state 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. 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, as defined by 15 U.S.C. section 1681a(p), 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. Nothing in this paragraph shall be construed to require the person to provide to any consumer reporting agency the names of the consumers entitled to receive the notice or any personal information relating to them.

State of Residence	New Hampshire continued
Enforcement/Private Cause of Action/ Penalties[3]	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. The New Hampshire attorney general's office shall enforce the provisions of this subdivision pursuant to RSA 358-A:4. The burden shall be on the person responsible for the determination under RSA 359-C:20, I to demonstrate compliance with this subdivision.

State of Residence	New Jersey
Statute	N.J. Stat. §§ 56:8-161, 163, 165 – 166
Definition of "Personal Information"	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 ID card number; (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 the person's financial account; or (4) username, 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.
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.
Analysis of Risk of Harm	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.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notice 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. 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.
Notifications to Regulators[2]	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. 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.
Enforcement/Private Cause of Action/ Penalties[3]	It shall be an unlawful practice and a violation of N.J. Stat. § 56:8-1 et seq. to willfully, knowingly, or recklessly violate sections §§ 56:8-161 – 164 of this amendatory and supplementary act.

State of Residence	New Mexico
Statute	N.M. Stat. §§ 57-12C-1 – 57-12C-12
Definition of "Personal Information"	First name or first initial and last name in combination with one or more of the following data elements, when the name and data elements are not protected through encryption or redacted or otherwise unreadable or unusable: 1) Social Security number; 2) driver's license number; 3) government-issued identification number; 4) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or 5) biometric data.
Definition of "Breach"	Unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that comprises the security, confidentiality or integrity of personal identifying information maintained by a person.
Analysis of Risk of Harm	Notification is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Notification shall be made in the most expedient time possible, but not later than 45 days following the discovery of the security breach. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.
Notifications to Regulators[2]	In the event notice is provided to more than 1,000 New Mexico residents, notice shall be given to the attorney general and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, no later than 45 days following discovery of the security breach. Notice shall include the number of New Mexico residents affected and include a copy of the notice that went to affected residents.
Enforcement/Private Cause of Action/ Penalties[3]	When the attorney general has a reasonable belief that a violation of the act occurred, the attorney general may bring an action in the name of the state. The court may issue an injunction and award damages for actual costs or losses, including consequential financial losses. If the court determines that a person violated the New Mexico Data Breach Notification Act knowingly or recklessly, the court may impose a civil penalty of the greater $25,000 or, in the case of failed notification, $10.00 per instance of failed notification up to a maximum of $150,000.

State of Residence	New York
Statute	N.Y. Gen. Bus. Law § 899-aa
Definition of "Personal Information"	"Personal Information" means any information concerning a natural person that, because of name, number, personal mark, or other identifier, can be used to identify such natural person. "Private Information" means either: (A) 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 ID card number; (3) account number, credit card number, 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 card number, 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; (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 (B) A username or email address in combination with a password or security question and answer that would permit access to an online account. *Note: Private information is the only information that triggers a breach notification in this state.
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.
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. 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 by an unauthorized person. 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 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 a username or email address in combination with a password or security question and answer that would permit access to an online account. Such a determination must be documented in writing and maintained for at least five (5) years. If the incident affects over 500 residents of New York, the person or business shall provide the written determination to the state attorney general within ten (10) days after the determination.

State of Residence	New York continued
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notice 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 system. Notification may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification shall be made after such law enforcement agency determines that such notification does not compromise such investigation.
Notifications to Regulators[2]	In the event that any 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. Such notice shall be made without delaying notice to affected New York residents. The person or business shall also provide a copy of the template of the notice sent to affected persons. In the event that more than five thousand 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. Any covered entity required to provide notification of a breach, including a breach of information that is not considered "private information," to the Secretary of Health and Human Services pursuant to HIPAA, shall provide such notification to the state attorney general within five (5) business days of notifying the Secretary.
Enforcement/Private Cause of Action/ Penalties[3]	Whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article he 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 ($5,000) or up to twenty thousand dollars ($20,000) per instance of failed notification, provided that the latter amount shall not exceed two hundred fifty thousand dollars ($250,000). The remedies provided by this section shall be in addition to any other lawful remedy available. No action may be brought under the provisions of this section unless such action is commenced within three (3) years after either the date on which the attorney general became aware of the violation, or the date that notice is sent to New York residents, whichever occurs first. In no event shall an action be brought after six (6) years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach.

State of Residence	North Carolina
Statute	N.C. Gen. Stat. §§ 75-61, 75-65
Definition of "Personal Information"	First name or first initial and last name in combination with identifying information: (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) electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names; (9) digital signatures; (10) any other numbers or information that can be used to access a person's financial resources; (11) biometric data; (12) fingerprints; (13) passwords; (14) parent's legal surname prior to marriage. *For purposes of this section, however, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.
Definition of "Breach"	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. *Note: "Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.
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?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notice 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. Notice 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. Notice 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.
Notifications to Regulators[2]	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. 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.
Enforcement/Private Cause of Action/ Penalties[3]	A violation of this section is a violation of G.S. 75-1.1. 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.

State of Residence	North Dakota
Statute	N.D. Cent. Code §§ 51-30-01 – 07
Definition of "Personal Information"	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.
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.
Analysis of Risk of Harm	NONE
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the integrity of the data system. The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification must be made after the law enforcement agency determines that the notification will not compromise the investigation.
Notifications to Regulators[2]	Any person who experiences a breach of the security system as provided in this section shall disclose to the attorney general by mail or email any breach of the security system which exceeds two hundred fifty individuals. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.
Enforcement/Private Cause of Action/ Penalties[3]	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.

State of Residence	Ohio
Statute	Ohio Rev. Code §§ 1349.19 – 192
Definition of "Personal Information"	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; or (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.
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
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?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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. 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.
Notifications to Regulators[2]	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 who 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.
Enforcement/Private Cause of Action/ Penalties[3]	The attorney general may conduct an investigation. There are various procedural rules. The attorney general shall have the exclusive authority to bring a civil action in a court of common pleas for appropriate relief, including a temporary restraining order, preliminary or permanent injunction, and civil penalties, if it appears that a person has failed or is failing to comply with this law. There are various civil penalties. See Ohio Rev. Code §§ 1349.191 - 192.

State of Residence	Oklahoma
Statute	Ok. Stat., Tit. 24, §§ 161–166
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 that relate to a resident of this state, when the data elements are neither encrypted nor redacted: (1) Social Security number; (2) driver license number or state identification card number issued in lieu of a driver 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 the financial accounts of a resident.
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 this state.
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?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Except as provided below 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. 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.
Notifications to Regulators[2]	NONE
Enforcement/Private Cause of Action/ Penalties[3]	A violation of this act that results in injury or loss to residents of this state may be enforced by the attorney general or a district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act. Except as otherwise provided, the attorney general or a district attorney shall have exclusive authority to bring action and may obtain either actual damages for a violation of this act or a civil penalty not to exceed $150,000.00 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

State of Residence	Oregon
Statute	Or. Rev. Stat. §§ 646A.600 - 646A.628
Definition of "Personal Information"	A) 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: (1) a consumer's Social Security number; (2) a consumer's driver's license number or state ID card number issued by the Department of Transportation; (3) a consumer's passport number or other ID number issued by the United States; (4) a consumer's financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account, 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; (5) 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; (6) a consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or (7) 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 (B) A username 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 username or means of identification; or (C) Any of the data elements described in (A) or (B) without the consumer's username, or the consumer's first name or first initial and last name, if: (1) encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and (2) the data element or combination of data elements would enable a person to commit identity theft against a consumer.
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.

State of Residence	Oregon continued
Analysis of Risk of Harm	A person does not need to notify consumers of a breach of security if, after an appropriate investigation or after consultation with relevant federal, state or local law enforcement agencies, the person reasonably determines that the consumers whose personal information was subject to the breach of security are unlikely to suffer harm. The person must document the determination in writing and maintain the documentation for at least five years.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Notice shall be made in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security. 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.
Notifications to Regulators[2]	Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to more than 1,000 consumers. If a breach affects 250 or more Oregon residents, notice must be given to the Oregon Attorney General, either in writing or electronically, and in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security. The person required to provide such notice must also submit 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.
Enforcement/Private Cause of Action/ Penalties[3]	In addition to all other penalties and enforcement provisions provided by law, any person who violates or who procures, aids, or abets in the violation of this statute shall be subject to a penalty of not more than $1,000 for every violation, which shall be paid to the General Fund of the State Treasury. Every violation is a separate offense and, in the case of a continuing violation, each day's continuance is a separate violation, but the maximum penalty for any occurrence shall not exceed $500,000. Civil penalties under this section shall be imposed as provided in Or. Rev. Stat. § 183.745. 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.

State of Residence	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.
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.
Analysis of Risk of Harm	An entity that maintains, stores or manages computerized data that includes personal information 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 resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Except as provided below or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. 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.
Notifications to Regulators[2]	Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals.
Enforcement/Private Cause of Action/ Penalties[3]	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. The office of attorney general shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

State of Residence	Rhode Island
Statute	R.I. Gen. Laws §§ 11-49.3-1–11-49.3-6
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 and the data elements are not encrypted or are in hard copy paper format: (1) Social Security number; (2) driver's license number, Rhode Island identification card number, or tribal identification number; (3) account number or credit or debit card number, in combination with any required security code, access code, password, or personal identification number that would permit access to an individual's financial account; (4) medical information, meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional or provider; or health insurance information, meaning an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual; or (5) e¬mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.
Definition of "Breach"	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.
Analysis of Risk of Harm	Notification shall be provided of any disclosure of personal information, or any breach of the security of the system, which poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notification shall be made in the most expedient time possible but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in this section and shall be consistent with the legitimate needs of law enforcement. The notification required by this section may be delayed if a federal, state, or local law enforcement agency determines that the notification will impede a criminal investigation. The federal, state, or local law enforcement agency must notify the municipal agency, state agency, or person of the request to delay notification without unreasonable delay.
Notifications to Regulators[2]	In the event that more than five hundred (500) Rhode Island residents are to be notified, the municipal agency, state agency, or person shall notify the attorney general and the major credit reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents.
Enforcement/Private Cause of Action/ Penalties[3]	Each reckless violation of this chapter is a civil violation for which a penalty of not more than one hundred dollars ($100) per record may be adjudged against a defendant. Each knowing and willful violation of this chapter is a civil violation for which a penalty of not more than two hundred dollars ($200) per record may be adjudged against a defendant. Whenever the attorney general has reason to believe that a violation of this chapter has occurred and that proceedings would be in the public interest, the attorney general may bring an action in the name of the state against the business or person in violation.

State of Residence	South Carolina
Statute	S.C. Code Ann. § 39-1-90
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 instead a driver's license; (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 account; or (4) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.
Definition of "Breach"	Unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident
Analysis of Risk of Harm	A person conducting business in South Carolina 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 this South Carolina whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, 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 of the information creates a material risk of harm to the resident.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notice shall be made 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. Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation The notification must be made after the law enforcement agency determines that it no longer compromises the investigation
Notifications to Regulators[2]	Notice, without unreasonable delay to the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals at one time.
Enforcement/Private Cause of Action/ Penalties[3]	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. A resident of South Carolina who is injured by a violation, 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.

State of Residence	South Dakota
Statute	SDCL §§ 22-40-19 - 22-40-26
Definition of "Personal Information"	"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. The term does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable. The Act also covers breaches of "Protected Information," regardless of whether individuals' names are involved, which includes: (1) a username 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. Thus, the Act will require disclosure of a breach of "Protected Information", even in the absence of an individual's name.
Definition of "Breach"	The unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder. 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.
Analysis of Risk of Harm	An information holder is not required to make a disclosure under this section if, following an appropriate investigation and notice to the state attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person. That determination must be documented in writing and maintained for at least three (3) years.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – based on factual circumstances where the information accessed is encrypted (without having access to the encryption key). In order to qualify as encrypted, computerized data must be rendered unusable, unreadable, or indecipherable either without the use of a decryption process or key or in accordance with the Federal Information Processing Standard (FIPS) 140-2 in effect on January 1, 2018.
Timing of Notification to Individuals	A disclosure shall be made within 60 days after discovering or receiving notification of the breach of system security, unless a longer period of time is required due a law enforcement agency's determination that the notification will impede a criminal investigation. If the notification is delayed, the notification must be provided within 30 days after the agency determines that notification will not compromise the investigation.
Notifications to Regulators[2]	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. If an information holder discovers circumstances that require notification to the attorney general pursuant to this Act the information holder shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice.
Enforcement/Private Cause of Action/ Penalties[3]	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 $10,000 per day, per violation. The attorney general also may recover attorney's fees and costs associated with bringing such an enforcement action.

State of Residence	Tennessee
Statute	Tenn. Code Ann. §§ 47-18-2105-2107
Definition of "Personal Information"	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 (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.
Definition of "Breach"	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.
Analysis of Risk of Harm	Any information holder 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 Tennessee whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances. Effective as of April 4, 2017, Tennessee amended its statute to clarify that its amendment in 2016 did not remove the encryption safe harbor. Instead, notification is not required if the data is encrypted in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2 and the encryption key has not been acquired by an unauthorized person.
Timing of Notification to Individuals	The disclosure shall be made immediately, but no later than forty-five (45) days from the discovery or notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made no later than forty-five (45) days after the law enforcement agency determines that it will not compromise the investigation.
Notifications to Regulators[2]	Notice, without unreasonable delay, to consumer reporting agencies and credit bureaus is required for any breach requiring notification to more than 1,000 individuals.
Enforcement/Private Cause of Action/ Penalties[3]	Any customer of an information holder who is a person or business entity, but who is not an agency of the state or any political subdivision of the state, and who is injured by a violation of this section, may institute a civil action to recover damages and to enjoin the person or business entity 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. A violation constitutes a violation of the Tennessee Consumer Protection Act. Notwithstanding any other law, a violation of this part shall be punishable by a civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (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.

State of Residence	Texas
Statute	Tex. Bus. & Com. Code §§ 521.002, 521.053, 521.151-152
Definition of "Personal Information"	"Sensitive Personal Information," which means: (A) 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: (1) Social Security number; (2) driver's license number or government-issued ID 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; or (B) Information that identifies an individual and relates to: (1) physical or mental health or condition of the individual; (2) provision of health care to the individual; or (3) payment for the provision of health care to the individual.
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.
Analysis of Risk of Harm	A person who conducts business in this state 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.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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 the breach occurred. A person may delay providing notice 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.
Notifications to Regulators[2]	A person who is required to disclose or provide notice of a breach shall notify the Texas Attorney General of that breach not later than the 60th day after the date on which the person determines that the breach occurred if the breach involves at least 250 residents. Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to more than 10,000 individuals at one time.
Enforcement/Private Cause of Action/ Penalties[3]	Liable for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring an action to recover the civil penalty imposed. In addition, a person who fails to take reasonable action to comply is liable for a civil penalty of not more than $100 for each individual to whom notification is due for each consecutive day that the person fails to take reasonable action to comply. Civil penalties may not exceed $250,000 for all individuals to whom notification is due after a single breach. If it appears to the attorney general that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the attorney general may bring an action in the name of the state against the person to restrain the violation by a temporary restraining order or by a permanent or temporary injunction.

State of Residence	Utah
Statute	Utah Code §§ 13-44-101 *et seq*.
Definition of "Personal Information"	First name or first initial and last name, combined with any one or more of the following data elements when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable: (1) Social Security number; (2)(a) financial account number, or credit or debit card number; and (b) any required security code, access code, or password that would permit access to the person's account; or (3) driver's license number or state ID card number.
Definition of "Breach"	Unauthorized acquisition of computerized data maintained by a person who compromises the security, confidentiality, or integrity of personal information.
Analysis of Risk of Harm	Notification is not required if after a reasonable and prompt investigation it is not revealed that misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	A person required to provide notification shall provide the notification in the most expedient time possible without unreasonable delay: (1) considering legitimate investigative needs of law enforcement; (2) after determining the scope of the breach of system security; and (3) after restoring the reasonable integrity of the system. A person may delay providing notification at the request of a law enforcement agency that determines that notification may impede a criminal investigation. A person who delays providing notification at the request of law enforcement shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.
Notifications to Regulators[2]	NONE
Enforcement/Private Cause of Action/ Penalties[3]	Civil fine of: (1) no greater than $2,500 for a violation or series of violations concerning a specific consumer; and (2) no greater than $100,000 in the aggregate for related violations concerning more than one consumer. The attorney general may seek injunctive relief to prevent future violations of this chapter.

State of Residence	Vermont
Statute	9 V.S.A. §§ 2430, 2435
Definition of "Personal Information"	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) a Social Security number; (2) a driver's license or non-driver 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) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords; (4) a password or personal ID number or other access code 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; (7) health records or records of a wellness program or similar program of health promotion or disease prevention; (8) a health care professional's medical diagnosis or treatment of the consumer; or (9) a health insurance policy number.
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 the data collector. *Note: "Login credentials" are defined as a consumer's username or email address, in combination with a password or an answer to a security question, that together permit access to an online account.
Analysis of Risk of Harm	Notice of a security breach is not required if misuse of personally identifiable information or login credentials is not reasonably possible and the data collector provides notice of its determination that the misuse of the personally identifiable information or login credentials is not reasonably possible and a detailed explanation for said determination is provided to the Vermont attorney general or to the Department of Financial Regulation in the event that the data collector is a person or entity licensed or registered with the Department. In determining whether personally identifiable information or login credentials have been acquired or are reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others: (1) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information; (2) indications that the information has been downloaded or copied; (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or (4) that the information has been made public. If the data collector subsequently obtains facts indicating that misuse of personally identifiable information or login credentials has occurred or is occurring, notice is required.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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.

State of Residence	Vermont continued
Notifications to Regulators[2]	Notification to the attorney general or the Department of Financial Regulation, as applicable, within 14 business days of discovery of the breach, consistent with the legitimate needs of the law enforcement agency or when the data collector provides notice to consumers pursuant to this section, whichever is sooner. If the date of the breach is unknown at the time notice is sent to the attorney general or to the Department, the data collector shall send the attorney general or the Department the date of the breach as soon as it is known. Unless otherwise ordered by a court of this state for good cause shown, a notice provided under subdivision (3)(B) shall not be disclosed to any person other than the Department, the authorized agent or representative of the attorney general, a state's attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data collector. Notice, without unreasonable delay, to all consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals. A data collector who, prior to the date of the breach, on a form and in a manner prescribed by the attorney general, had sworn in writing to the attorney general that it maintains written policies and procedures to maintain the security of personally identifiable information or login credentials and respond to a breach in a manner consistent with Vermont law shall notify the attorney general of the date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers. If a security breach is limited to an unauthorized acquisition of login credentials, a data collector is only required to provide notice of the security breach to the attorney general or Department of Financial Regulation, as applicable, if the login credentials were acquired directly from the data collector or its agent.
Enforcement/Private Cause of Action/ Penalties[3]	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.

State of Residence	Virginia
Statute	Va. Code § 18.2-186.6; Va. Code § 32.1-127.1:05; Va. Code § 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; or (5) military identification number. **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. However, the statute does not apply to 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 publicly available information, or from federal, state, or local government records lawfully made available to the general public.
Definition of "Breach"	Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of 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. **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 employee or agent of an entity for the purposes of the entity is not a breach of the security system, provided that the medical information is not used for a purpose other than a lawful purpose of the entity or subject to further unauthorized disclosure.
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 has caused or will cause, identity theft or another fraud to any resident of Virginia.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Notice, without unreasonable delay, to any affected resident of Virginia. 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. Notice may be delayed if, after the individual or entity notifies a law- enforcement agency, the 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 shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security. **Medical Information-Specific Statute** Notice, without unreasonable delay, to the subject of the medical information, and any affected resident of the Commonwealth. Other provisions set forth above in this section also apply.

State of Residence	Virginia continued
Notifications to Regulators[2]	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. Notice may be delayed if, after the individual or entity notifies a law-enforcement agency, the 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 shall be made without unreasonable delay after the law- enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security. Notice to the attorney general and consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals. 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 the discovery or notification of unauthorized access and acquisition of unencrypted and unredacted computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person, and causes, or the employer or payroll provider reasonably believes has caused or will cause, identity theft or other fraud. With respect to employers, this requirement applies only to information regarding the employer's employees, and does not apply to information regarding the employer's customers or other non-employees. The employer or payroll service provider must provide the Attorney General with the name and federal employer identification number of the employer that may be affected by the compromise in confidentiality. 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. **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.
Enforcement/Private Cause of Action/ Penalties[3]	The attorney general may bring an action to address violations of this section, and 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. Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section. 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. 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. **Medical Information-Specific Statute** No private right of action. The statute does not explicitly provide for regulatory enforcement.

State of Residence	Washington
Statute	Wash. Rev. Code § 19.255.010 *et seq.*
Definition of "Personal Information"	"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 data elements: (1) Social Security number; (2) driver's license number or Washington ID card number; (3) account number or credit card number or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account or any other numbers or information that can be used to access a person's financial account; (4) full date of birth; (5) private key that is unique to an individual and that is used to authenticate or sign an electronic record; (6) student, military, or passport identification number; (6) health insurance policy number or health insurance identification number; (7) 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 (8) biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual; or (B) Any of the data elements above, alone or combined, without the individual's first name or first initial and last name if: (1) encryption, redaction, or other methods have not be applied to render the element(s) unusable and (2) the element(s) would enable a person to commit identity theft against a consumer; or (C) A username or email address in combination with a password or security questions and answers that would permit access to an online account.
Definition of "Breach"	Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.
Analysis of Risk of Harm	Notice is not required if the breach is not reasonably likely to subject consumers to a risk of harm.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notice shall be made in the most expedient time possible and without unreasonable delay, no more than thirty (30) calendar days after the breach was discovered, unless the delay is at the request of law enforcement or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Notification 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. Notification shall be made after the law enforcement agency determines that it will not compromise the investigation.
Notifications to Regulators[2]	Any person or business required to notify more than 500 Washington residents as a result of a single breach shall notify the attorney general of the breach no more than thirty (30) days after the breach was discovered. Notification 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. Notification shall be made after the law enforcement agency determines that it will not compromise the investigation.

State of Residence	Washington continued
Enforcement/Private Cause of Action/ Penalties[3]	The 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 section. A violation is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act, Wash. Rev. Code 19.86. Any consumer injured by a violation of this section may institute a civil action to recover damages. Any person or business that violates, proposes to violate, or has violated this section may be enjoined. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

State of Residence	West Virginia
Statute	W.V. Code § 46A-2A-101 *et seq.*
Definition of "Personal Information"	First name or first initial and last name 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; 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.
Definition of "Breach"	Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of West Virginia.
Analysis of Risk of Harm	Notice is required if there is a reasonable belief that unauthorized access or acquisition has caused or will cause identity theft or other fraud to any West Virginia resident.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Except as provided below 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 notice shall be made without unreasonable delay. 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.
Notifications to Regulators[2]	Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals.
Enforcement/Private Cause of Action/ Penalties[3]	Failure to comply with the notice provisions constitutes an unfair or deceptive act of practice, which may be enforced by the attorney general. The attorney general shall have exclusive authority to bring action. No civil penalty may be assessed in an action unless the court finds that the defendant has engaged in a course of repeated and willful violations of this article. No civil penalty shall exceed $150,000 per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation. A violation of this article by a licensed financial institution shall be enforceable exclusively by the financial institution's primary functional regulator.

State of Residence	Wisconsin
Statute	Wis. Stat. § 134.98
Definition of "Personal Information"	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) Social Security number; (2) driver's license number or state ID number; (3) 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, as defined in s. 939.74(2d)(a); or (5) individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.
Definition of "Breach"	(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. (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.
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.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The notice shall be made 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. A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required for any period of time and the notification process required shall begin at the end of that time period. If an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.
Notifications to Regulators[2]	Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to 1,000 or more individuals.
Enforcement/Private Cause of Action/ Penalties[3]	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.

State of Residence	Wyoming
Statute	Wyo. Stat. §§ 40-12-501, 40-12-502
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 element, 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.
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.
Analysis of Risk of Harm	If the definition of "breach" is not met, then notice is not required. Residents must be notified of a breach of the security system when, after a good faith, reasonable and prompt investigation, the individual or commercial entity determines that the misuse of personally identifying information about a Wyoming resident has occurred or is reasonably likely to occur.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	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. The notification required may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation.
Notifications to Regulators[2]	NONE
Enforcement/Private Cause of Action/ Penalties[3]	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.

U.S. TERRITORIES	
State of Residence	**Guam**
Statute	9 Guam Code §§ 48.10 - .80
Definition of "Personal Information"	The first name, or first initial, and last name in combination with and linked to any one or more of the following data elements that relate to a resident of 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.
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 Guam.
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?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Except as provided below 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. *Note: 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. 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.
Notifications to Regulators[2]	NONE
Enforcement/Private Cause of Action/ Penalties[3]	A violation of this Chapter that results in injury or loss to residents of Guam may be enforced by the office of the attorney general. Except as provided by § 48.40 of this Chapter, the office of the attorney general shall have exclusive authority to bring action and may obtain either actual damages for a violation of this Chapter 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.

State of Residence	Puerto Rico
Statute	P.R. Laws tit. 10, § 4051 *et seq.*
Definition of "Personal Information"	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: (1) Social Security number; (2) driver's license number, voter's identification or other official identification; (3) bank or financial account numbers of any type with or without passwords or access code that may have been assigned; (4) names of users and passwords or access codes to public or private information systems; (5) medical information protected by the HIPAA; (6) tax information; and (7) work-related evaluations. 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.
Definition of "Breach"	"Breach" 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.
Analysis of Risk of Harm	Any entity that is the owner or custodian of a database that includes personal information of citizens of 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.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	Clients 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.
Notifications to Regulators[2]	Within a non-extendable term of ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information.
Enforcement/Private Cause of Action/ Penalties[3]	The Secretary may impose fines of five hundred dollars ($500) up to a maximum of five thousand dollars ($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.

State of Residence	U.S. Virgin Islands
Statute	V.I. Code tit. 14, § 2208 *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: (1) Social Security number; (2) driver's license number; (3) 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.
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 the person or business.
Analysis of Risk of Harm	Any person or business that conducts business in the Virgin Islands, and 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.
Safe Harbor for Data that is Encrypted, Unreadable, Unusable, or Redacted?[1]	Yes – in certain situations depending on the factual circumstances.
Timing of Notification to Individuals	The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The notification required by this section may be delayed if 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.
Notifications to Regulators[2]	NONE
Enforcement/Private Cause of Action/ Penalties[3]	Any customer injured by a violation of this title may commence a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

About Foley

Foley & Lardner LLP looks beyond the law to focus on the constantly evolving demands facing our clients and their industries. With more than 1,100 lawyers in 24 offices across the United States, Mexico, Europe, and Asia, Foley approaches client service by first understanding our clients' priorities, objectives, and challenges. We work hard to understand our clients' issues and forge long-term relationships with them to help achieve successful outcomes and solve their legal issues through practical business advice and cutting-edge legal insight. Our clients view us as trusted business advisors because we understand that great legal service is only valuable if it is relevant, practical and beneficial to their businesses.

FOLEY

FOLEY & LARDNER LLP

AUSTIN | BOSTON | BRUSSELS | CHICAGO | DALLAS | DENVER | DETROIT | HOUSTON | JACKSONVILLE | LOS ANGELES | MADISON | MEXICO CITY | MIAMI
MILWAUKEE | NEW YORK | ORLANDO | SACRAMENTO | SAN DIEGO | SAN FRANCISCO | SILICON VALLEY | TALLAHASSEE | TAMPA | TOKYO | WASHINGTON, D.C.