

# State Data Breach Notification Laws



Please note that state data breach notification laws change frequently. The recommended actions an entity should take if it experiences a security event, incident or breach vary depending on the specific facts and circumstances. This Chart is merely a summary of some basic state notification requirements that are applicable to persons or entities who "own" or "license" data. **For example, this Chart does not cover:**

- Requirements for entities that maintain data rather than "own" or "license" data. (Note: entities that maintain data are generally required to notify the owner/licensor.)
- Exceptions to the law (e.g., sometimes health care providers, data brokers, financial institutions, insurers, etc. are partially or fully excluded).
- Exceptions to the law regarding good faith acquisition of personal information by an employee or agent of an entity for a legitimate purpose of the entity if the employee or agent does not use the personal information for a purpose unrelated to a legitimate purpose of the entity and does not make further unauthorized disclosure of the personal information.
- Any secondary guidance materials issued by state agencies.
- The manner in which an entity provides notification (e.g., via e-mail, U.S. Mail, etc.).
- The specifics regarding what constitutes public, encrypted, redacted, unreadable, or unusable data.

This Chart is current as of **April 14, 2018**.

For more information about state data breach notification laws, or other data security matters, please contact your Quarles & Brady Attorney, or:

**John Barlament** ([john.barlament@quarles.com](mailto:john.barlament@quarles.com) | 414.277.5727).

**Heather Buchta** ([heather.buchta@quarles.com](mailto:heather.buchta@quarles.com) | 602.229.5228).

**Linda Emery** ([linda.emery@quarles.com](mailto:linda.emery@quarles.com) | 414.277.3038).

**Meghan O'Connor** ([meghan.oconnor@quarles.com](mailto:meghan.oconnor@quarles.com) | 414.277.5423).

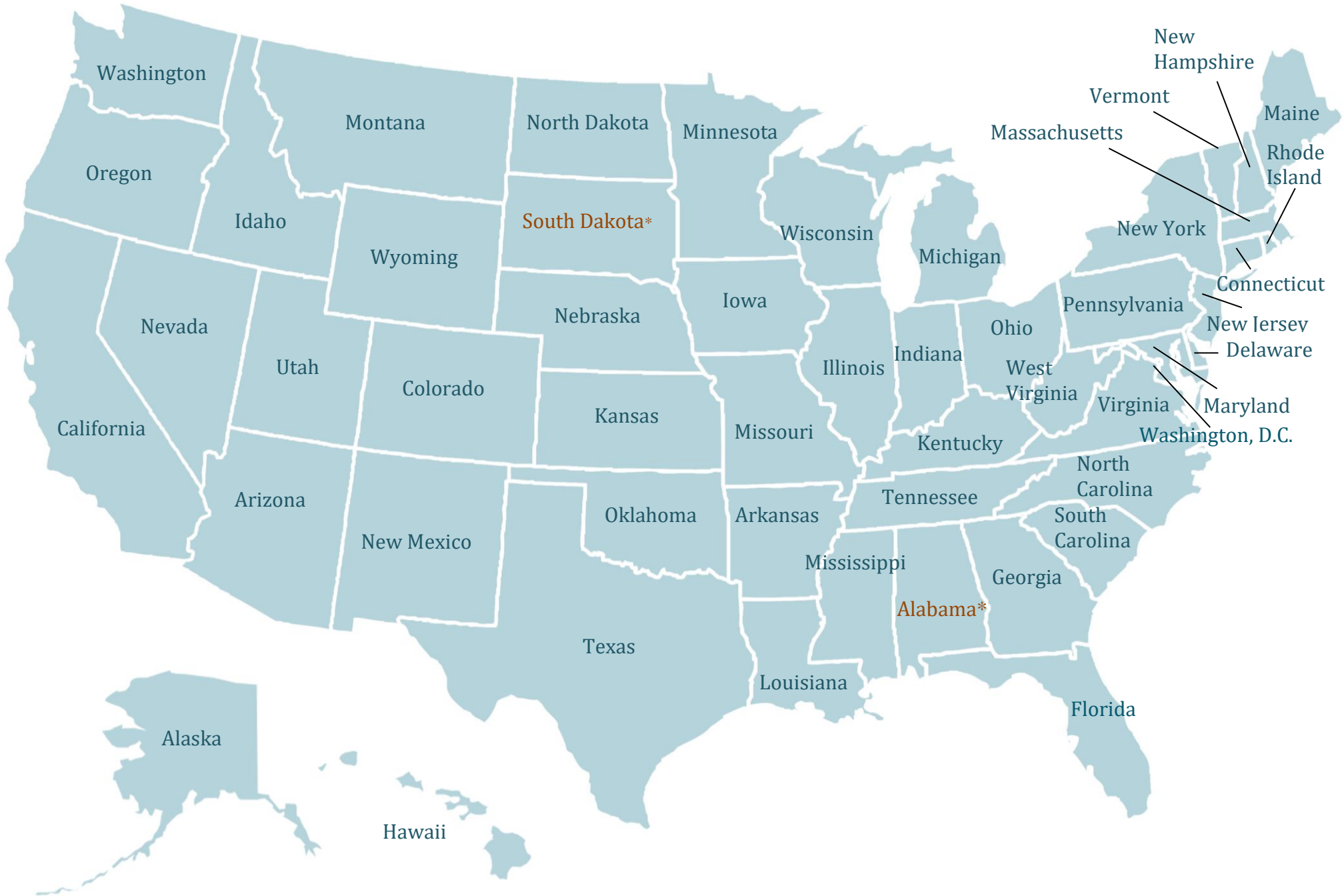
**Receipt and/or review of this Chart does not create an attorney-client relationship.**

**Updates:** We intend to continue updating this Chart at no charge. If you would like to receive updates, please send an email to

**Linda Emery** ([linda.emery@quarles.com](mailto:linda.emery@quarles.com)).



*This Chart is current as of April 14, 2018.*



*\*Breach notification law enacted but not yet effective.*

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/<br>Enforcement <sup>2</sup>  | Statute   |
|--------------------|--|--|---|--|--|---|---|
| Alabama            | A covered entity that is not a third-party agent that determines during a required investigation that, as a result of a breach of security, sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates, shall give notice of the breach to each individual. | Except as provided in paragraph b., 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) | 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. | 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 as required under the Act. Except as delayed for law enforcement purposes, 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.<br><br>If a federal or state law enforcement agency determines that notice to individuals required under this section would interfere with a criminal investigation or national security, the notice shall be delayed upon the receipt of written request of the law enforcement agency for a period that the law enforcement | If the number of individuals a covered entity is required to notify exceeds 1,000, the entity shall provide written notice of the breach to the Attorney General as expeditiously as possible and without unreasonable delay. Except as delayed for law enforcement purposes, 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.<br><br>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 | A violation of the notification provisions of this act is an unlawful trade practice under the Alabama Deceptive Trade Practices Act, Chapter 19, Title 8, Code of Alabama 1975, but does not constitute a criminal offense under Section 8-19-12, Code of Alabama 1975 (listing deceptive acts or practices). The Attorney General shall have the exclusive authority to bring an action for civil penalties under this act.<br><br>(1) A violation of this act does not establish a private cause of action under Section 8-19-10, Code of Alabama 1975 (deceptive trade practices). Nothing in this act may otherwise be construed to affect any right a person may have at common law, by statute, or otherwise.<br><br>(2) Any covered entity or third-party agent who is knowingly engaging in or has knowingly engaged in a violation of the notification provisions of this act will be subject to the penalty provisions set | *Note: S.B. 318 establishes a data breach law. It becomes effective June 1, 2018. |

<sup>1</sup> See also Analysis of Risk of Harm/Identity Theft/Materiality Column.

<sup>2</sup> These penalties are limited to those referenced in the data breach laws cited in this Chart. There may be other potentially applicable penalties and enforcement actions depending upon the circumstances.

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information   | Definition of "Breach" | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute |
|--------------------|---|--|------------------------|---|---|--|---------|
|                    |   | <p>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. (6) A user name 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.</p> <p>(B) 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. (2) Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements</p> |                        | <p>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.</p> | <p>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.</p> | <p>out in Section 8–19–11, Code of Alabama 1975 (deceptive trade practices penalties). For the purposes of this act, knowingly shall mean willfully or with reckless disregard in failing to comply with the notice requirements of Sections 5 and 6. Civil penalties assessed under Section 8–19–11, Code of Alabama 1975 (deceptive trade practices penalties), shall not exceed five hundred thousand dollars (\$500,000) per breach.</p> <p>Notwithstanding any remedy available under subdivision (2) of subsection (a) of this section, a covered entity that violates the notification provisions of this act shall be liable for a civil penalty of not more than five thousand dollars (\$5,000) per day for each consecutive day that the covered entity fails to take reasonable action to comply with the notice provisions of this act.</p> <p>The office of the Attorney General shall have the exclusive authority to bring an action for damages in a representative capacity on behalf of any named</p> |         |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information  | Definition of "Breach" | Timing of Individual Notice Requirements | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup>   | Statute |
|--------------------|---|---|------------------------|--|--|---|---------|
|                    |   | <p>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.</p> |                        |  |  | <p>individual or individuals. In such an action brought by the office of the Attorney General, recovery shall be limited to actual damages suffered by the person or persons, plus reasonable attorney's fees and costs.</p> <p>To the extent that notification is required under this act as the result of a breach experienced by a third-party agent, a failure to inform the covered entity of the breach shall subject the third-party agent to the fines and penalties set forth in the act.</p> <p>All government entities are exempt from any civil penalty authorized by this act; provided, however, the Attorney General may bring an action against any state, county, or municipal official or employee, in his or her official capacity, who is subject to this act for any of the following: (1) To compel the performance of his or her duties under this act. (2) To compel the performance of his or her ministerial acts under this act. (3) To enjoin him or her from acting in bad faith, fraudulently, beyond his</p> |         |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/<br>Enforcement <sup>2</sup>   | Statute                                 |
|--------------------|---|--|---|--|--|--|---|
|                    |   |  |   |  |  | or her authority, or under mistaken interpretation of the law.   |   |
| Alaska             | 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. | 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:<br><br>(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<br><br>(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 | 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.<br><br>Acquisition includes acquisition by:<br>(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. | 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.<br><br>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. | 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. | 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. When private action, limited to actual economic damages.<br><br>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. | Alaska Stat. § 45.48.010 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/<br>Enforcement <sup>2</sup>   | Statute   |
|--------------------|---|---|--|--|--|--|---|
|                    |   | <p>identification numbers, or other access codes for financial accounts.</p> <p>"Personal code" means a security code, an access code, a personal identification number, or a password.</p>   |  |  |  |  |   |
| Arizona            | <p>The person shall conduct a reasonable investigation to promptly determine if there has been a breach of the security system. If the investigation results in a determination that there has been a breach in the security system, the person shall notify the individuals affected. A person is not required to disclose a breach of the security of the system if the person or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur.</p> | <p>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 encrypted, redacted or secured by any other method rendering the element unreadable or unusable: (1) The individual's social security number; (2) The individual's number on a driver license issued pursuant to § 28-3166 or number on a non-operating identification license issued pursuant to § 28-3165; (3) The individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account.</p> | <p>An unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information and that causes or is reasonably likely to cause substantial economic loss to an individual.</p> | <p>The notice shall be made in the most expedient manner possible and without unreasonable delay subject to the needs of law enforcement and any measures necessary to determine the nature and scope of the breach, to identify the individuals affected or to restore the reasonable integrity of the data system.</p> <p>The notification may be delayed if a law enforcement agency advises the person that the notification will impede a criminal investigation. The person shall make the notification after the law enforcement agency determines that it will not compromise the investigation.</p> | NONE   | <p>This law may only be enforced by the attorney general. The attorney general may bring an action to obtain actual damages for a willful and knowing violation of this section and a civil penalty not to exceed \$10,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.</p> | <p>Ariz. Rev. Stat. § 18-545</p> <p>HB2154</p> <p>*Note: H.B. 2154 modifies these provisions. It becomes effective on the 91st day after the date on which the session of the legislature enacting it is adjourned <i>sine die</i>.</p> |
| Arkansas           | <p>Notification is not required if, after a reasonable</p>  | <p>An individual's first name or first initial and his or her last name in</p>  | <p>Unauthorized acquisition of computerized data that</p>  | <p>The disclosure shall be made in the most expedient time and</p>   | NONE   | <p>Any violation of this chapter is punishable by action of the Attorney</p>   | <p>Ark. Code § 4-110-101 <i>et seq.</i></p>   |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute                        |
|--------------------|---|--|--|---|---|---|--------------------------------|
|                    | investigation, the person or business determines that there is no reasonable likelihood of harm to customers. | combination with any one or more of the following data elements when either the name or the data element is not encrypted or redacted:<br>(1) Social security number; (2) Driver's license number or Arkansas identification card number;<br>(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; and<br>(4) Medical information, meaning any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional. | compromises the security, confidentiality, or integrity of personal information maintained by a person or business.  | 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.<br><br>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. |   | General under the provisions of § 4-88-101 <i>et seq.</i> (deceptive trade practice).   |                                |
| California         | NONE  | (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:<br>(1) Social security number; (2) Driver's license number or  | Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. | 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  | 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 | 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. | Cal. Civ. Code §§ 1798.80, .82 |



| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute                           |
|--------------------|---|--|---|--|---|--|-----------------------------------|
|                    |   | <p>California identification card number;</p> <p>(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;</p> <p>(4) Medical information;</p> <p>(5) Health insurance information;</p> <p>(6) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.</p> <p>(B) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.</p> |   | <p>the reasonable integrity of the data system.</p> <p>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.</p> | <p>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.</p>  |  |                                   |
| Colorado           | <p>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 prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or the</p> | <p>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:</p>  | <p>Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.</p> | <p>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.</p>   | <p>If an individual or commercial entity is required to notify more than 1,000 Colorado residents of a breach of the security of the system, the individual or commercial entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a</p> | <p>The 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 an individual or a</p> | <p>Colo. Rev. Stat. § 6-1-716</p> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                     |
|--------------------|--|--|---|---|--|--|-----------------------------|
|                    | commercial entity shall give notice as soon as possible to the affected Colorado resident unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur.                     | (1) Social security number; (2) Driver's license number or 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. |   | 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 individual or commercial entity that conducts business in Colorado not to send notice required by this section. Notice required by this section shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation and has notified the individual or commercial entity that conducts business in Colorado that it is appropriate to send the notice required by this section. | nationwide basis, as defined by 15 U.S.C. sec. 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. | commercial entity subject to this section from compliance with all other applicable provisions of law.   |                             |
| Connecticut        | 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 | 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     | 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 | 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  | 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.  | Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General. | Conn. Gen. Stat. § 36a-701b |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute  |
|--------------------|---|---|--|--|---|--|--|
|                    | individuals whose personal information has been acquired and accessed.  | combination with any required security code, access code or password that would permit access to an individual's financial account.   | technology that renders the personal information unreadable or unusable.   | nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system.<br><br>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. |   |  |  |
| Delaware           | Any person who conducts business in this State 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 this State whose personal information was breached or is | 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 that individual: (1) Social security number; (2) Driver's license number or state or federal identification number; (3) Account number, or credit card number, or debit card number, in combination | The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.<br><br>The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information is not a | Notice must be made in without unreasonable delay but not later than 60 days after determination of the breach of security, except in the following situations: (1) A shorter time is required under federal law; (2) A law enforcement agency determines that the notice will impede a criminal investigation and such law enforcement agency has   | 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 Attorney General. | Pursuant to the enforcement duties and powers of the Director of Consumer Protection of the Department of Justice under Chapter 25 of Title 29, 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 | Del. Code Ann. tit. 6 § 12B-101 <i>et seq.</i> |

| State of Residence   | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute                            |
|----------------------|---|--|--|---|---|--|------------------------------------|
|                      | <p>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.</p> <p>*"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.</p> | <p>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 healthcare professional, or deoxyribonucleic acid profile; (7) Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person; (8) Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes; (9) An individual taxpayer identification number.</p> | <p>breach of security to the extent that personal information contained therein is encrypted, unless such unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.</p> | <p>made a request of the person that the notice be delayed. Any such delayed notice must be made after such law enforcement agency determines that notice will not compromise the criminal investigation and so notifies the person of such determination; (3) When a person otherwise required to provide notice, could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of this State was included in a breach of security, such person must provide the notice to such residents as soon as practicable after the determination that the breach of security included the personal information of such residents, unless such person provides or has provided substitute notice.</p> |   | <p>damages resulting from a violation, or both. The provisions of this chapter are not exclusive and do not relieve a person subject to this chapter from compliance with all other applicable provisions of law.</p> <p>Nothing in this chapter may be construed to modify any right which a person may have at common law, by statute, or otherwise.</p> |                                    |
| District of Columbia | NONE  | (A) An individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements:<br>(1) Social security   | Unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the   | The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law  | 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 | Any District of Columbia resident injured by a violation of this subchapter may institute a civil action to recover actual damages, the costs of the action,   | D.C. Code § 28-3851 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>   | Statute |
|--------------------|---|--|--|---|--|---|---------|
|                    |   | <p>number; (2) Driver's license number or District of Columbia Identification Card number; or (3) Credit card number or debit card number;</p> <p>or</p> <p>(B) Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.</p> | <p>security, confidentiality, or integrity of personal information maintained by the person or business.</p> | <p>enforcement and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>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.</p> | <p>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.</p> | <p>and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering.</p> <p>The Attorney General may petition the Superior Court of the District of Columbia for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by District of Columbia residents as a consequence of the violation of this subchapter. In an action under this subsection, the Attorney General may recover a civil penalty not to exceed \$100 for each violation, the costs of the action, and reasonable attorney's fees. Each failure to provide a District of Columbia resident with notification in accordance with this section shall constitute a separate violation.</p> <p>The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.</p> |         |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute              |
|--------------------|---|--|---|---|--|--|----------------------|
| Florida            | 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. | (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 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.<br><br>or<br><br>(B) A user name or email address, in | Unauthorized access of data in electronic form containing personal information. | 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.<br><br>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.<br><br>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 | Notice to Department of Legal Affairs required for notification to 500 or more 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.<br><br>A covered entity may provide the Department of Legal Affairs with supplemental information regarding a breach at any time.<br><br>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, | A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the Department of Legal Affairs under s. 501.207 against a covered entity or third-party agent.<br><br>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:<br><br>(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.<br><br>(2) If the violation continues for more than 180 days, in an amount not to exceed \$500,000.<br><br>The civil penalties for failure to notify provided in this paragraph apply per breach and not per individual affected by the breach.<br><br>All penalties collected pursuant to this subsection shall be deposited into the General Revenue Fund. | Fla. Stat. § 501.171 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>                               | Statute                                   |
|--------------------|---|---|---|---|---|---|---|
|                    |   | <p>combination with a password or security question and answer that would permit access to an online account.</p> <p>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.</p>   |   | <p>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.</p>   | <p>15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.</p>  | <p>This section does not establish a private cause of action.</p> |   |
| Georgia            | NONE  | <p>(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</p> | <p>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.</p> | <p>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.</p> <p>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</p> | <p>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.</p> | NONE  | <p>Ga. Code § 10-1-910 <i>et seq.</i></p> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality            | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                                 |
|--------------------|--|---|--|--|--|--|---|
|                    |  | <p>identification numbers or other access codes;</p> <p>or</p> <p>(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.</p>   |  | not compromise the investigation.  |  |  |   |
| Hawaii             | If the definition of "breach" is not met, then notice is not required. | <p>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:</p> <p>(1) Social security number; (2) Driver's license number or Hawaii identification card number; or</p> <p>(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.</p> | <p>Unauthorized access to and acquisition of unencrypted or redacted 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.</p> <p>*Note: "records" means any material on</p> | <p>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.</p> <p>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</p> | <p>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.</p> | <p>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.</p> <p>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</p> | Haw. Rev. Stat. § 487N-1 <i>et seq.</i> |



| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup>   | Statute                               |
|--------------------|--|--|--|--|--|---|---------------------------------------|
|                    |  |  | which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.   | 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. |  | reasonable attorneys' fees to the prevailing party.<br><br>The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this State.  |                                       |
| Idaho              | A city, county or state agency, 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, | 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 | Illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons maintained by an agency, individual or a commercial entity. | 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.<br><br>Notice may be delayed if a law enforcement agency advises the agency, individual or commercial entity that    | NONE   | In any case in which an agency's, commercial entity's or individual's primary regulator has reason to believe that an agency, individual or 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 | Idaho Code § 28-51-104 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup>   | Statute   |
|--------------------|--|---|---|--|--|---|---|
|                    | <p>individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident.</p> <p>Also, if the definition of "breach" is not met, then notice is not required.</p> | <p>permit access to a resident's financial account.</p>   |   | <p>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, individual or commercial entity that notification will no longer impede the investigation.</p>  |  | <p>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.</p> |   |
| Illinois           | NONE   | <p>(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</p> | <p>Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.</p> | <p>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.</p> <p>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</p> | NONE   | <p>A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.</p>  | <p>815 Ill. Comp. Stat. 530/5 <i>et. seq.</i></p> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information   | Definition of "Breach" | Timing of Individual Notice Requirements        | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup> | Statute |
|--------------------|---|--|------------------------|---|--|-------------------------------------|---------|
|                    |   | <p>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 healthcare professional, including such information provided to a website or mobile application; (5) 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 any medical information in an individual's health insurance application and claims history, including any appeals records; (6) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;</p> |                        | <p>longer interfere with the investigation.</p> |  |                                     |         |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute                                       |
|--------------------|---|---|--|--|---|---|---|
|                    |   | <p>or</p> <p>(B) A user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.</p>   |  |  |   |   |   |
| Indiana            | <p>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:</p> <p>(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;</p> <p>if the data base owner knows, should know,</p> | <p>(A) A Social security number that is not encrypted or redacted;</p> <p>or</p> <p>(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; (4) A financial account number or debit card number in combination with a security code, password, or access code that would permit</p> | <p>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.</p> | <p>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:</p> <p>(a) impede a criminal or civil investigation; or</p> | <p>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.</p> <p>If a data base owner makes a disclosure to individuals, the data base owner shall also</p> | <p>A person that is required to make a disclosure or notification and that fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general under this chapter. 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.</p> <p>The attorney general may bring an action under this chapter to obtain any or all of the following: (1) An</p> | <p>Ind. Code § 24-4.9-1-1 <i>et. seq.</i></p> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute   |
|--------------------|--|---|--|--|--|--|---|
|                    | 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.  | access to the person's account.   | 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. | (b) jeopardize national security.<br><br>A person required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after:<br>(1) delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or<br>(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. | disclose the breach to the attorney general.   | 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:<br>(a) the investigation of the deceptive act; and<br>(b) maintaining the action.  |   |
| Iowa               | 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 | 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 | Unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.<br><br>"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   | 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.   | 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 following discovery of such breach of security, or receipt of notification by any person who maintains | 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.<br><br>The rights and remedies available under this section are cumulative to each other and to any | Iowa Code § 715C.1 <i>et seq.</i><br><br>*Note: SF 2177 modifies these provisions. It becomes effective July 1, 2018. |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute                             |
|--------------------|--|--|--|---|---|--|-------------------------------------|
|                    | must be maintained for five years.   | 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. | person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information.                 | 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. | personal information on behalf of another person, 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. | other rights and remedies available under the law.   |                                     |
| Kansas             | A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information shall, | 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   | Unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal | 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   | In the event that a person discovers the circumstances requiring notification pursuant to this section of more than 1,000 consumers at one time, the person shall also notify, without unreasonable   | 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 | Kan. Stat. § 50-7a01 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                         |
|--------------------|--|---|--|---|--|--|---------------------------------|
|                    | <p>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.</p> <p>Also, if the definition of "breach" is not met, then notice is not required.</p> | <p>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.</p>            | <p>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.</p>  | <p>determine the scope of the breach and to restore the reasonable integrity of the computerized data system.</p> <p>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.</p> | <p>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.</p>  | <p>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.</p> <p>Insurance companies: the insurance commissioner shall have the sole authority to enforce the provisions of this section.</p> |                                 |
| Kentucky           | <p>If the definition of "breach" is not met, then notice is not required.</p>  | <p>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</p> | <p>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</p> | <p>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.</p>   | <p>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</p> | <p>NONE</p>  | <p>Ky. Rev. Stat. § 365.732</p> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/<br>Enforcement <sup>2</sup>  | Statute                                 |
|--------------------|--|---|---|---|--|---|---|
|                    |  | with any required security code, access code, or password to permit access to an individual's financial account.  | 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.  | 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.   | defined by 15 U.S.C. sec. 1681a, of the timing, distribution, and content of the notices.  |   |   |
| Louisiana          | Notification under this title is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers. | 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 element is not encrypted or redacted: (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. | The compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person. | The notification 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, prevent further disclosures, and restore the reasonable integrity of the data system.<br><br>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 notice to Louisiana citizens is required, the person or agency 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 Louisiana citizens affected by the breach. Notice to the attorney general shall be timely if received within 10 days of distribution of notice to Louisiana citizens. | 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.<br><br>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 shall be deemed a separate violation. | La. Rev. Stat. § 51:3071 <i>et seq.</i> |
| Maine              | If any person becomes aware of a breach of the security of the system, the person  | (A) An individual's first name or initial and last name in combination with any one or more of  | Unauthorized acquisition, release or use of an individual's computerized data that  | The notices must be made as expediently as possible and without unreasonable delay,   | If a person discovers a breach of the security of the system that requires notification to   | The appropriate state regulators within the Department of Professional and  | 10 Me. Rev. Stat. § 1346 <i>et seq.</i> |



| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute |
|--------------------|---|--|---|---|---|---|---------|
|                    | 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. | 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<br><br>(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. | includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person. | 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.<br><br>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. | 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.<br><br>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. | Financial Regulation shall enforce this chapter for any person that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other persons.<br><br>A person that violates this chapter commits a civil violation and is subject to one or more of the following:<br><br>(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;<br><br>(2) Equitable relief; or<br><br>(3) Enjoinment from further violations of this chapter.<br><br>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 | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute   |
|--------------------|--|--|---|---|---|---|---|
| Maryland           | <p>A business that owns or licenses computerized data that includes personal information of an individual residing in the State, 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 of the individual has been or will be misused as a result of the breach. If, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the business shall notify the individual of the breach.</p> <p>If after the investigation is concluded, the business determines that notification is not required, the business shall maintain records that reflect its determination for three years after the determination is made.</p> | <p>(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, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government; (2) A driver's license number or State identification card number; (3) An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account; (4) Health information, including information about an individual's mental health; (5) A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an</p> | <p>Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business.</p> | <p>The notice shall be given as soon as reasonably practicable, but not later than 45 days after the business concludes the investigation.</p> <p>Notice may be delayed:<br/>(1) If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or<br/>(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.</p> <p>If notification is delayed by law enforcement, notification shall be given as soon as reasonably practicable, but not later than 30 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.</p> | <p>Prior to giving the individual notification required by law, and subject to permissible delay, a business shall provide notice of a breach of the security of a system to the Office of the Attorney General.</p> <p>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.</p> | <p>A violation:</p> <p>(1) Is an unfair or deceptive trade practice within the meaning of the Consumer Protection Act;<br/>and<br/>(2) Is subject to the enforcement and penalty provisions contained in the Consumer Protection Act.</p> | <p>Md. Code Com. Law § 14-3501 <i>et seq.</i></p> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information  | Definition of "Breach" | Timing of Individual Notice Requirements | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup> | Statute |
|--------------------|---|---|------------------------|--|--|-------------------------------------|---------|
|                    |   | <p>employer that is self-insured, that permits access to an individual's health information; or</p> <p>(6) Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account.</p> <p>or</p> <p>(B) A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account.</p> <p>*"Health information" means any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996 regarding an individual's medical history, medical condition, or medical treatment or diagnosis.</p> |                        |  |  |                                     |         |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality            | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute                                |
|--------------------|--|---|---|--|---|--|--|
| Massachusetts      | If the definition of "breach" is not met, then notice is not required. | 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. | <p>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.</p> <p>*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.</p> | <p>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.</p> <p>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</p> | <p>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.</p> <p>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 of</p> | 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. | Mass. Gen. Laws 93H § 1 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                         |
|--------------------|---|---|---|--|--|--|---------------------------------|
|                    |   |   |   | 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.   | consumer affairs and business regulation.  |  |                                 |
| Michigan           | 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 | 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 license number or state personal identification card number; (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. | 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. | 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:<br><br>(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. | 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.<br><br>This does not apply if the following is met:<br><br>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. | A person that 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.<br><br>The aggregate liability of a person for civil fines for multiple violations that arise from the same security breach shall not exceed \$750,000.<br><br>This does not affect the availability of any civil remedy for a violation of state or federal law. | Mich. Comp. Laws §§ 445.63, .72 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                       |
|--------------------|---|---|--|---|--|--|-------------------------------|
|                    | <p>in encrypted form by a person with unauthorized access to the encryption key.</p> <p>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.</p> |   |  | <p>(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.</p>                           |  |  |                               |
| Minnesota          | NONE  | <p>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:<br/>(1) Social security number; (2) Driver's license number or Minnesota identification</p> | <p>Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the business.</p> | <p>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.</p> <p>Notification may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.</p> | <p>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.</p> | <p>The attorney general shall enforce this section under section 8.31 (additional duties of attorney general).</p> | <p>Minn. Stat. § 325E.61.</p> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup>   | Statute               |
|--------------------|---|---|---|---|--|---|-----------------------|
|                    |   | 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.  |   |   |  |   |                       |
| Mississippi        | 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. | 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. | 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. | 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.<br><br>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 | NONE   | 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. | Miss. Code § 75-24-29 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute                   |
|--------------------|--|--|---|---|---|--|---------------------------|
|                    |  |  |   | notification will not compromise the criminal investigation or national security and so notifies the person of that determination.  |   |  |                           |
| Missouri           | 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. | 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 | Unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. | The disclosure notification shall be:<br>(1) Made without unreasonable delay;<br>(2) Consistent with the legitimate needs of law enforcement, as provided in this section; and<br>(3) Consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.<br><br>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 | 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. | 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. | Mo. Rev. Stat. § 407.1500 |



| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality                   | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute   |
|--------------------|---|---|---|--|--|--|---|
|                    |   | <p>permit access to an individual's financial account; (5) Medical information; or (6) Health insurance information.</p>  |   | <p>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.</p>   |  |  |   |
| Montana            | <p>If the definition of "breach" is not met, then notice is not required.</p> | <p>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</p> | <p>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.</p> | <p>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.</p> <p>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.</p> | <p>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.</p> <p>Any person or business that is required to issue a notification pursuant to this section shall simultaneously submit an electronic copy of</p> | <p>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).</p> <p>The provisions of 30-14-111(3) and (4) and 30-14-112 through 30-14-115 apply to this part.</p> <p>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.</p> | <p>Mont. Code §§ 30-14-1701-1702, 1704-1705</p> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute                                 |
|--------------------|---|--|--|---|---|--|---|
|                    |   | identification number issued by the United States internal revenue service.  |  |   | 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. |  |   |
| Nebraska           | 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. | Personal information means either of the following:<br><br>(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:<br>(1) Social security number; (2) Motor | Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. | 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.<br><br>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 | 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.  | The Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of Neb. Rev. Stat. § 87-803 (Breach of security; investigation; notice to resident; notice to Attorney General).<br><br>A violation of section 7 of this act shall be considered a violation of section 59-1602 (Unfair competition; practices; unlawful) and be subject to the Consumer Protection Act and any other law which | Neb. Rev. Stat. § 87-801 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality            | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>   | Statute                                 |
|--------------------|--|--|--|--|--|---|---|
|                    |  | <p>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</p> <p>(B) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.</p> |  | as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation  |  | provides for the implementation an enforcement of section 59-1602. A violation of section 7 of this act does not give rise to a private cause of action.  |   |
| Nevada             | If the definition of "breach" is not met, then notice is not required. | A natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (1) Social security number; (2) Driver's license number,   | Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. | 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 | 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. | 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 | Nev. Rev. Stat. 603A.010 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information   | Definition of "Breach" | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup>  | Statute |
|--------------------|---|--|------------------------|--|--|--|---------|
|                    |   | <p>driver authorization card number or 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 the person's financial account; (4) A medical identification number or a health insurance identification number; (5) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.</p> <p>The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state or local governmental records.</p> |                        | <p>the reasonable integrity of the system data.</p> <p>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.</p> |  | <p>person to obtain a temporary or permanent injunction against the violation.</p> |         |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute                          |
|--------------------|---|---|---|---|---|---|----------------------------------|
| New Hampshire      | 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. | 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. | Unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. | The person shall notify the affected individuals as soon as possible as required under this subdivision.<br><br>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. | 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.<br><br>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 | 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.<br><br>The New Hampshire attorney general's office shall enforce the provisions of this subdivision pursuant to RSA 358-A:4.<br><br>The burden shall be on the person responsible | N.H. Rev. Stat. §§ 359-C:19–C:21 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute                                |
|--------------------|---|---|--|---|---|---|--|
|                    |   |   |  |   | 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. | for the determination under RSA 359-C:20, I to demonstrate compliance with this subdivision.  |  |
| New Jersey         | 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. | 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; 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 | 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 | The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.<br><br>The notification required by this section shall be delayed if a law | 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   | It shall be an unlawful practice and a violation of N.J. Stat. § 56:8-1 <i>et seq.</i> to willfully, knowingly or recklessly violate sections §§ 56:8-161 – 164 of this amendatory and supplementary act. | N.J. Stat. §§ 56:8-161, 163, 165 – 166 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute  |
|--------------------|--|--|--|--|--|--|--|
|                    |  | <p>access to the person's financial account.</p> <p>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.</p> | <p>information unreadable or unusable.</p>   | <p>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.</p> | <p>handling, which may include dissemination or referral to other appropriate law enforcement entities.</p> <p>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.</p> |  |  |
| New Mexico         | <p>Notification to affected New Mexico residents 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.</p> | <p>An individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered</p>      | <p>Unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data that compromises the</p> | <p>Notification shall be made in the most expedient time possible, but not later than forty-five calendar days following discovery of the security breach, except the notification may be delayed: (1) if a law enforcement agency determines that the</p>   | <p>A person that is required to issue notification of a security breach pursuant to this act to more than 1,000 New Mexico residents as a result of a single security breach shall notify the office of the attorney general and</p>   | <p>When the attorney general has a reasonable belief that a violation of the Data Breach Notification Act has occurred, the attorney general may bring an action on the behalf of individuals and in the name of the state</p> | <p>N.M. Stat. Ann. § 57-12C-1 <i>et seq.</i></p> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                     |
|--------------------|---|---|---|---|--|--|-----------------------------|
|                    |   | 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, meaning a record generated by automatic measurements of an identified individual's fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account. | security, confidentiality or integrity of personal identifying information maintained by a person.  | notification will impede a criminal investigation; or (2) as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.  | major 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 security breach in the most expedient time possible, and no later than forty-five calendar days, except the notification may be delayed: (1) if a law enforcement agency determines that the notification will impede a criminal investigation; or (2) as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system. | alleging a violation of this act.<br><br>In any action filed by the attorney general pursuant to the Data Breach Notification Act, the court may:<br><br>(1) issue an injunction; and<br><br>(2) award damages for actual costs or losses, including consequential financial losses.<br><br>If the court determines that a person violated this act knowingly or recklessly, the court may impose a civil penalty of the greater of twenty-five thousand dollars (\$25,000) or, in the case of failed notification, ten dollars (\$10.00) per instance of failed notification up to a maximum of one hundred fifty thousand dollars (\$150,000). |                             |
| New York           | 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:<br>(1) indications that the | "Personal Information" - any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.<br><br>"Private Information" - personal information consisting of any   | Unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. | 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. | 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   | 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   | N.Y. Gen. Bus. Law § 899-aa |



| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information  | Definition of "Breach" | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute |
|--------------------|--|---|------------------------|---|--|--|---------|
|                    | <p>information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;</p> <p>(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.</p> | <p>information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) Social security number; (2) Driver's license number or non-driver ID card 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.</p> <p>*Note: private information is the only information that triggers a breach notification in this state.</p> |                        | <p>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.</p> | <p>notice shall be made without delaying notice to affected New York residents.</p> <p>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.</p> | <p>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.</p> <p>Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, provided that the latter amount shall not exceed one hundred fifty thousand dollars.</p> <p>The remedies provided by this section shall be in addition to any other lawful remedy available.</p> <p>No action may be brought under the provisions of this section unless such action is commenced within two years immediately after the date of the act</p> |         |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality            | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute                         |
|--------------------|--|---|---|--|---|--|---------------------------------|
|                    |  |   |   |  |   | complained of or the date of discovery of such act.  |                                 |
| North Carolina     | If the definition of "breach" is not met, then notice is not required. | <p>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.</p> <p>* For purposes of this section, however, personal information</p> | <p>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.</p> <p>*Note: "Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.</p> | <p>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.</p> <p>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.</p> <p>Notice shall be provided without unreasonable delay after the law enforcement agency</p> | <p>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.</p> <p>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</p> | <p>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.</p> <p>Causes of action arising under this Article may not be assigned.</p> | N.C. Gen. Stat. §§ 75-61, 75-65 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                          |
|--------------------|---|--|--|--|--|--|----------------------------------|
|                    |   | 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.  |  | communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.  | timing, distribution, and content of the notice.   |  |                                  |
| North Dakota       | NONE  | 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, | 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. | 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.<br><br>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. | Any person that 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. | 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. | N.D. Cent. Code §§ 51-30-01 – 07 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality            | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute                         |
|--------------------|--|--|--|--|---|---|---------------------------------|
|                    |  | 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. |  |  |   |   |                                 |
| Ohio               | If the definition of "breach" is not met, then notice is not required. | 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        | 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 | 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. | 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 | The attorney general may conduct an investigation. There are various procedural rules.<br><br>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.<br><br>The court shall impose a civil penalty as follows: | Ohio Rev. Code §§ 1349.19 – 192 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality            | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                        |
|--------------------|--|--|--|---|--|--|--------------------------------|
|                    |  | 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. |  | 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. | shall a person that is required to make a notification required by this division delay any disclosure or notification in order to make the notification required by this division. | If the person has intentionally or recklessly failed to comply with the applicable section, (1) a civil penalty of up to \$1,000 for each day the person fails to comply with the section for each day of the first sixty days that the person fails to comply with the section, (2) a civil penalty of up to \$5,000 for each day commencing with the sixty-first day and continuing through the ninetieth day that the person fails to comply with the section, and, (3) for each day commencing with the ninety-first day that the person has failed to comply with the section, a civil penalty of up to \$10,000 for each such day the person fails to comply with the section.<br><br>The rights and remedies that are provided under this section are in addition to any other rights or remedies that are provided by law. |                                |
| Oklahoma           | If the definition of "breach" is not met, then notice is not required. | 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             | Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or | 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,   | NONE   | 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  | Ok. Stat., Tit. 24, §§ 161-166 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute  |
|--------------------|---|---|--|---|---|--|--|
|                    |   | 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.                            | 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. | the disclosure shall be made without unreasonable delay.<br><br>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. |   | unlawful practice under the Oklahoma Consumer Protection Act.<br><br>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.                     |  |
| Oregon             | 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 | (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 | Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains.  | The notice shall be made in the most expeditious manner possible, without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures that are necessary to determine sufficient contact information for the affected consumer, determine the scope of the breach of security and restore the reasonable integrity, security and confidentiality of the personal information.  | Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to more than 1,000 consumers.<br><br>Notice in the most expeditious manner possible, either written or electronically, to the Attorney General if the number of consumers to whom the person must send notice exceeds 250. | 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.<br><br>Every violation is a separate offense and, in the case of a continuing violation, each day's continuance is a separate violation, but the | Or. Rev. Stat. §§ 646A.602, 646A.604, 646A.624<br><br>*Note: S.B. 1551 modifies these provisions. It becomes effective June 2, 2018. |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality     | Personal Information  | Definition of "Breach" | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup>   | Statute |
|--------------------|---|---|------------------------|---|--|---|---------|
|                    | writing and maintain the documentation for at least five years. | 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; (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 |                        | A person that owns or licenses personal information may delay notifying a consumer of a breach of security 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. |  | <p>maximum penalty for any occurrence shall not exceed \$500,000.</p> <p>Civil penalties under this section shall be imposed as provided in Or. Rev. Stat. § 183.745.</p> <p>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.</p> |         |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                            |
|--------------------|--|--|--|--|--|--|------------------------------------|
|                    |  | <p>diagnosis or treatment of the consumer.</p> <p>OR</p> <p>(B) Any of the data elements described in (A) without 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.</p>                                     |  |  |  |  |                                    |
| Pennsylvania       | 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. | 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 | 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. | 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.<br><br>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. | Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals. | 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 <i>et seq.</i> known as the Unfair Trade Practices and Consumer Protection Law.<br><br>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. | 73 Pa. Stat. § 2301 <i>et seq.</i> |



| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute                                       |
|--------------------|---|---|--|--|---|---|---|
|                    |   | access to an individual's financial account.  |  | Notification shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.   |   |   |   |
| Rhode Island       | 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. | 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:<br><br>(1) Social security number; (2) Driver's license number, or Rhode Island identification card number or tribal identification number; (3) Account number, credit or debit card number, in combination with any required security code, access code, password or personal identification number that would 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 | 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. | 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.<br><br>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. | 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. | 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.<br><br>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.<br><br>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. | R.I. Gen'l Law, tit. 11-49.3.1 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute                  |
|--------------------|--|---|--|---|---|---|--------------------------|
|                    |  | 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.   |  |   |   |   |                          |
| South Carolina     | 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 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 | 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, or 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 | 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. | The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.<br><br>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 | If a business provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in 15 USC Section 1681a(p), of the timing, distribution, and content of the notice. | 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.<br><br>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; | S.C. Code Ann. § 39-1-90 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute  |
|--------------------|---|--|--|---|---|--|--|
|                    | information creates a material risk of harm to the resident.  | 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.   |  | longer compromises the investigation  |   | (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.   |  |
| South Dakota       | An information holder is not required to make a disclosure if, following an appropriate investigation and notice to the attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person. | "Personal information" means a person's first name or first initial and last name, in combination with any one or more of the following data elements: (1) Social security number; (2) Driver 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; or (5) An identification number assigned to a person by the person's employer in combination with any required security code, | 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 disclosure shall be made not later than sixty (60) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement. A notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, the notification shall be made not later than thirty (30) days after the law enforcement agency determines that notification will not compromise the criminal investigation. | 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 two hundred fifty (250) residents of this state.<br><br>If an information holder discovers circumstances that require notification pursuant to individuals, 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, | The attorney general may prosecute each failure to disclose under the provisions of this Act as a deceptive act or practice under § 37-24-6. In addition to any remedy provided under chapter 37-24, the attorney general may bring an action to recover on behalf of the state a civil penalty of not more than ten thousand dollars per day per violation. The attorney general may recover attorney's fees and any costs associated with any action brought under this section. | *Note: S.B. 62 establishes a data breach law. It becomes effective July 1, 2018. |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute                         |
|--------------------|---|---|---|---|---|--|---------------------------------|
|                    |   | <p>access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes.</p> <p>"Protected information" includes: (1) A user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and (2) Account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account.</p> |   |   | and content of the notice.  |  |                                 |
| Tennessee          | The information holder shall disclose the breach of system security to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. | First name or first initial and last name, in combination with any one or more of the following data elements: (1) Social security number; (2) Driver license number; or (3) Account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.  | Acquisition of: unencrypted computerized data, or encrypted computerized data and the encryption key, by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. | <p>The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement.</p> <p>The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is</p> | Notice, without unreasonable delay, to all consumer reporting agencies and credit bureaus is required for any breach requiring notification to more than 1,000 individuals at one time. | 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 information holder from further action in violation of this section. The rights and remedies available under this section are cumulative to each other | Tenn. Code §§ 47-18-2105 - 2107 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>   | Statute  |
|--------------------|---|---|---|---|---|---|--|
|                    |   |   |   | delayed, it must be made no later than forty-five (45) days after the law enforcement agency determines that notification will not compromise the investigation.                        |   | and to any other rights and remedies available under law.<br><br>A violation constitutes a violation of the Tennessee Consumer Protection Act.<br><br>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. |  |
| Texas              | 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 | "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:<br>(1) Social security | Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data | Disclosure shall be made as quickly as possible, except as provided below or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. | Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to more than 10,000 individuals at one time. | 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.  | Tex. Bus. & Com. Code §§ 521.002, 521.053, 521.151-152 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup>   | Statute                               |
|--------------------|---|---|--|---|--|---|---------------------------------------|
|                    | 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.   | 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;<br><br>or<br><br>(B) Information that identifies an individual and relates to:<br>(1) Physical or mental health or condition of the individual;<br>(2) Provision of health care to the individual; or<br>(3) Payment for the provision of health care to the individual. | that is encrypted if the person accessing the data has the key required to decrypt the data.   | 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. |  | 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.<br><br>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. |                                       |
| Utah               | 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. | 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:  | Unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. | 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  | NONE   | Civil penalty 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.  | Utah Code §§ 13-44-101 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>   | Statute                |
|--------------------|--|--|---|--|--|---|------------------------|
|                    |  | (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.  |   | the breach of system security; and (3) after restoring the reasonable integrity of the system.<br><br>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. |  | The attorney general may seek: (1) injunctive relief to prevent future violations of this chapter; and (2) attorney fees and costs.   |                        |
| Vermont            | Notice of a security breach is not required if misuse of personal information is not reasonably possible and the data collector provides notice of its determination that the misuse of the personal information is not reasonably possible and a detailed explanation for said determination to the Vermont Attorney General or to the Department of Financial Regulation | First name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: (1) Social security number; (2) Motor vehicle operator's license number or nondriver ID card; | 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 maintained by the data collector. | 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.  | 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.<br><br>If the date of the breach is unknown at the time notice is sent to the | 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.<br><br>The Attorney General may refer the matter to the State's Attorney in an appropriate case. | 9 V.S.A. §§ 2430, 2435 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach" | Timing of Individual Notice Requirements | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup> | Statute |
|--------------------|---|---|------------------------|--|---|-------------------------------------|---------|
|                    | <p>in the event that the data collector is a person or entity licensed or registered with the Department.</p> <p>In determining whether personally identifiable information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others:</p> <p>(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;</p> <p>(2) indications that the information has been downloaded or copied;</p> <p>(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.</p> <p>If the data collector subsequently obtains facts indicating that</p> | <p>(3) Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;</p> <p>(4) Account passwords or personal ID numbers or other access codes for a financial account.</p> |                        |  | <p>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.</p> <p>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.</p> <p>Notice, without unreasonable delay, to all consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals.</p> <p>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</p> |                                     |         |



| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"   | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute               |
|--------------------|--|--|--|---|---|--|-----------------------|
|                    | misuse of the personal information has occurred or is occurring, notice is required.   |  |  |   | maintains written policies and procedures to maintain the security of personally identifiable information 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.  |  |                       |
| Virginia           | 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. | 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; or (3) Financial 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 a resident's financial accounts. | 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. | Notice, without unreasonable delay, to any affected resident of Virginia.<br><br>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.<br><br>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, without unreasonable delay, to the Attorney General if any Virginia residents must be notified.<br><br>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.<br><br>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. | 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.<br><br>A violation of this section by a state-chartered or licensed financial institution shall be enforceable exclusively by the | Va. Code § 18.2-186.6 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information   | Definition of "Breach" | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute |
|--------------------|---|--|------------------------|---|---|--|---------|
|                    |   | <p>*Note: See Notice Requirements to Officials/Agencies regarding 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.</p> |                        | <p>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.</p> | <p>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.</p> <p>Notice to the Attorney General and consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals.</p> <p>Notwithstanding any other provision of this section, any employer or payroll service provider that owns or licenses computerized data relating to income tax withheld pursuant to Article 16 (§ 58.1-460 et seq.) of Chapter 3 of Title 58.1 shall notify the Office of 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</p> | <p>financial institution's primary state regulator.</p> <p>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.</p> |         |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute                                     |
|--------------------|---|---|---|--|--|--|---|
|                    |   |   |   |  | <p>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.</p> <p>With respect to employers, this subsection applies only to information regarding the employer's employees, and does not apply to information regarding the employer's customers or other non-employees. Such employer or payroll service provider shall provide the Office of the Attorney General with the name and federal employer identification number of the employer that may be affected by the compromise in confidentiality.</p> |  |   |
| Washington         | Notice is not required if the breach is not reasonably likely to subject consumers to a risk of harm. | First name or first initial and last name in combination with any one or more of the following data elements: | Unauthorized acquisition of data that compromises the security, confidentiality, or | The notice must be made in the most expedient time possible and without unreasonable delay, no more than | Any person or business required to notify more than 500 Washington residents as a result of a single breach, shall, by   | The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons | Wash. Rev. Code § 19.255.010 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup>  | Penalties/ Enforcement <sup>2</sup>  | Statute                               |
|--------------------|--|---|---|--|---|--|---------------------------------------|
|                    |  | (1) Social security number; (2) Driver's license number or Washington ID card number; or (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. | integrity of personal information maintained by the person or business.   | <p>forty-five calendar days after the breach was discovered, unless 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.</p> <p>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.</p> | <p>the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. The person or business shall also provide to the Attorney General the number of Washington consumers affected by the breach, or an estimate if the exact number is not known.</p> <p>Notice to the Attorney General must be made in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered, unless 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.</p> | <p>residing in the state, to enforce this section.</p> <p>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.</p> <p>Any consumer injured by a violation of this section may institute a civil action to recover damages.</p> <p>Any person or business that violates, proposes to violate, or has violated this section may be enjoined.</p> <p>The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.</p> |                                       |
| West Virginia      | 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 | 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;   | Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of | 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   | Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to more than 1,000 individuals.  | <p>Failure to comply with the notice provisions constitutes an unfair or deceptive act of practice, which may be enforced by the Attorney General.</p> <p>The Attorney General shall have exclusive</p>  | W.V. Code § 46A-2A-101 <i>et seq.</i> |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality  | Personal Information   | Definition of "Breach"  | Timing of Individual Notice Requirements  | Notice Requirements to Officials/Agencies <sup>1</sup>   | Penalties/ Enforcement <sup>2</sup>  | Statute             |
|--------------------|--|--|---|---|--|--|---------------------|
|                    | any West Virginia resident.  | (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.  | 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.   | without unreasonable delay.<br><br>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.<br><br>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.     |  | 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.<br><br>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.<br><br>A violation of this article by a licensed financial institution shall be enforceable exclusively by the financial institution's primary functional regulator. |                     |
| Wisconsin          | 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. | 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 | (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 | 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.<br><br>A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to | Notice, without unreasonable delay, to consumer reporting agencies is required for any breach requiring notification to 1,000 or more individuals. | 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.  | Wis. Stat. § 134.98 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality   | Personal Information  | Definition of "Breach"  | Timing of Individual Notice Requirements   | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup>   | Statute                            |
|--------------------|---|---|---|--|--|---|------------------------------------|
|                    |   | 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.   | subject of the personal information.<br><br>(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. | 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.  |  |   |                                    |
| Wyoming            | If the definition of "breach" is not met, then notice is not required.<br><br>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. | 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:<br>(1) Address;<br>(2) Telephone number;<br>(3) Social security number; (4) Driver's license number;<br>(5) 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; (6) Tribal ID;<br>(7) Federal or state | 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.  | 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.<br><br>The notification required may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation. | NONE   | 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. | Wyo. Stat. §§ 40-12-501, 40-12-502 |

| State of Residence | Analysis of Risk of Harm/<br>Identity Theft/<br>Materiality | Personal Information  | Definition of "Breach" | Timing of Individual Notice Requirements | Notice Requirements to Officials/Agencies <sup>1</sup> | Penalties/ Enforcement <sup>2</sup> | Statute |
|--------------------|---|---|------------------------|--|--|-------------------------------------|---------|
|                    |   | <p>government issued ID;</p> <p>(8) Shared secrets or security tokens that are known to be used for data based authentication;</p> <p>(9) Username or email address, in combination with a password or security question and answer that would permit access to an online account;</p> <p>(10) Birth or marriage certificate; (11) Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;</p> <p>(12) Health insurance information;</p> <p>(13) Unique biometric data; (14) Individual Taxpayer Identification Number.</p> |                        |  |  |                                     |         |