STATE DATA SECURITY BREACH NOTIFICATION LAWS

Please note: This chart is for informational purposes only and does not constitute legal advice or opinions regarding any specific facts relating to specific data breach incidents. You should seek the advice of experienced legal counsel when reviewing options and obligations in responding to a particular data security breach.

Laws and regulations change quickly in the data security arena. This chart is current as of June 1, 2018.

The general definition of “personal information” used in the majority of statutes is: An individual’s first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver’s license number or state-issued identification card number, and (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account. The general definition generally applies to computerized data that includes personal information and usually excludes publicly available information that is lawfully made available to the general public from federal, state or local governments or widely distributed media. When a statute varies from this general definition, it will be pointed out and underlined in the chart.

The term “security breach” is used in this chart to capture the concept variably described in state statutes as a “security breach,” “breach of the security,” “breach of the security system,” or “breach of the security of the system,” among other descriptions.

This chart provides general information and not legal advice regarding any specific facts or circumstances. For more information about security breach notification laws, or other privacy and data security matters, please contact the Mintz Levin attorney with whom you work, or Cynthia Larose, CIPP/US, CIPP/E (cjarose@mintz.com | 617.348.1732), Dianne Bourque (dbourque@mintz.com | 617.348.1614), Susan Foster, CIPP/E (sfoster@mintz.com | +44.20.7776.7330), Brian Lam, CIPP/US, FIP, CISSP (bhlam@mintz.com | 858.314.1583) or Ari Moskowitz, CIPP/US (amoskowitz@mintz.com | 202.434.7379).

For entities doing business in Texas, be sure to review the relevant Texas law. Please note that rules applicable to state agencies, government bodies and other public institutions are not discussed in this chart.

- Alabama
- Alaska
- Arkansas
- Arizona
- California
- Colorado
- Connecticut
- Delaware
- District of Columbia
- Florida
- Georgia

- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan

- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota

- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Texas
- Utah
- Virginia
- Vermont

- Washington
- Wisconsin
- West Virginia
- Wyoming
- Puerto Rico
- Virgin Islands
**Important Definitions:**

"Breach of Security" or "Breach" means 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.

**Third party recipients:**
Third parties maintaining personal information on behalf of a covered entity must notify covered entity about a breach and cooperate as necessary to allow covered entity to comply with statute. The covered entity must satisfy all further notification obligations under the statute.

**Other Obligations:**
Any covered entity that must notify more than 1,000 residents at one time of a security breach is also required to notify the Attorney General and consumer reporting agencies without unreasonable delay, but no later than forty-five (45) days following the discovery of the breach.

**Encryption Safe Harbor:**
Statute not applicable if the personal information that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted.

**Other exemptions:**
Expiration for good faith acquisition by an employee or agent of covered entity so long as personal information is used for a legitimate purpose of employer and is not subject to further unauthorized disclosure.

**Penalties:**
A determination of no likelihood of harm: Does not require notification to Attorney General.

Violations by non-governmental entities constitute unlawful trade practices under the Alabama Deceptive Trade Practice Act, Chapter 19, Title 8, Code of Alabama 1975. Such entities are liable for civil penalties up to $5,000 per day for each consecutive day the entity fails to take reasonable action to comply with notice provisions, with the total civil penalty not to exceed $500,000. Damages awarded under AL Section 8-19-11 are limited to actual damages suffered by the person(s) plus attorney’s fees and costs.

**Private Cause of Action:**
No.

**Enforcement:**
Enforcement by Attorney General only.
<table>
<thead>
<tr>
<th>Information</th>
<th>Alaska</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Covered</strong></td>
<td>Personal information of Alaska residents.</td>
</tr>
<tr>
<td><strong>Important Definitions</strong></td>
<td>- &quot;Security Breach&quot; means an unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of the personal information maintained.</td>
</tr>
<tr>
<td>- &quot;Acquisition&quot; means any method of acquisition, including by photocopying, facsimile, or other paper-based method, or a device, including a computer, that can read, write, or store information that is represented in numerical form.</td>
<td></td>
</tr>
<tr>
<td><strong>Subject to statute:</strong></td>
<td>Any person doing business in Alaska and any person with more than ten employees.</td>
</tr>
<tr>
<td><strong>Third party recipients:</strong></td>
<td>Third parties maintaining personal information on behalf of a covered entity must notify covered entity about a breach and cooperate as necessary to allow covered entity to comply with statute. The covered entity must satisfy all further notification obligations under the statute.</td>
</tr>
<tr>
<td><strong>Written or electronic notice must be provided:</strong></td>
<td>To victims of a security breach in the most expeditious time possible and without unreasonable delay, unless law enforcement agency determines that disclosure will interfere with a criminal investigation (in which case notification delayed until authorized by law enforcement).</td>
</tr>
<tr>
<td><strong>Important definitions:</strong></td>
<td>Substitute notice is available by means prescribed in the statute if costs to exceed $150,000, affected class exceeds 300,000 persons, or covered entity has insufficient contact information.</td>
</tr>
<tr>
<td><strong>Notice not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a reasonable likelihood of harm to the consumers whose personal information was acquired:</strong></td>
<td>The determination must be documented in writing and maintained for five years.</td>
</tr>
<tr>
<td><strong>Other Obligations:</strong></td>
<td>Any covered entity that must notify more than 1,000 residents at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies. This section does not apply to entities subject to Title V of the Gramm-Leach-Bliley Act of 1999 (&quot;GLBA&quot;).</td>
</tr>
<tr>
<td><strong>Encryption Safe Harbor:</strong></td>
<td>Statute not applicable if the personal information that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted.</td>
</tr>
<tr>
<td><strong>Safe Harbor:</strong></td>
<td>Safe harbor not available if the personal information is encrypted but the encryption key has been accessed or acquired.</td>
</tr>
<tr>
<td><strong>Other Exemptions:</strong></td>
<td>Exemption for good faith acquisition by an employee or agent of covered entity so long as personal information is used for a legitimate purpose of employer and is not subject to further unauthorized disclosure.</td>
</tr>
<tr>
<td><strong>Penalties:</strong></td>
<td>A determination of no likelihood of harm: Requires written notification to Attorney General.</td>
</tr>
<tr>
<td><strong>Private Cause of Action:</strong></td>
<td>A waiver of the statute is void and unenforceable.</td>
</tr>
<tr>
<td><strong>Encryption Safe Harbor / Other Exemptions</strong></td>
<td>Violations by non-governmental entities constitute unfair or deceptive acts or practices under AS 45.50.471 - 45.50.561. Such entities are liable for civil penalties up to $500 per resident who was not properly notified, with the total civil penalty not to exceed $50,000.</td>
</tr>
<tr>
<td><strong>Notification to Regulator / Waiver</strong></td>
<td>Damages awarded under AS 45.50.531 are limited to actual economic damages that do not exceed $500, and damages awarded under AS 45.50.537 are limited to actual economic damages.</td>
</tr>
<tr>
<td><strong>State / Link to Statute</strong></td>
<td>Return to Index of States</td>
</tr>
<tr>
<td><strong>Information Covered / Important Definitions</strong></td>
<td>Click here to review text of statute.</td>
</tr>
<tr>
<td><strong>Covered Entities</strong></td>
<td>Third Party Recipients</td>
</tr>
<tr>
<td><strong>Notice Procedures &amp; Timing / Other Obligations</strong></td>
<td></td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Arizona</td>
<td>Information covered: Personal information of Arizona residents in computerized data maintained by a covered entity is subject to notification requirements under the statute.</td>
</tr>
</tbody>
</table>

**Important definitions:**

- “Security Breach” means an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a covered entity as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual.
- “Encrypted” means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.
- “Redact” means altering or truncating data such that no more than the last four digits of a social security number, driver license number, nonoperating identification license number, financial account number or credit or debit card number is accessible as part of the personal information.

**Liability and Penalties:**

- Definition includes: a private key used to authenticate or sign an electronic record; individual health insurance identification number, medical information; passport number; a taxpayer identification number or PIN issued by the IRS; or unique biometric data used to access online accounts.

- **Notices:**
  - Written, electronic or telephonic notices must be provided within the most expedient manner possible and without unreasonable delay but not later than forty-five (45) days following the determination of the breach, unless a law enforcement agency advises the covered entity that notification will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).
  - **Specific requirements for the form and content of notice:**
    - Substitute notice is available by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information.
    - Notice not required if the covered entity or law enforcement entity determines that a breach has not occurred or is not reasonably likely to occur (i.e. the breach does not materially compromise the security or confidentiality of the personal information maintained and has not caused or is not reasonably likely to cause substantial economic loss to an individual).

- **Other Obligations:**
  - Any covered entity that must notify more than 1,000 residents at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.

- **Encryption Safe Harbor:**
  - Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or secured by method rendering data unreadable or unusable.
  - Other exemptions:
    - Exemption for good faith acquisition by an employee or agent of a covered entity so long as personal information not used for a purpose unrelated to the covered entity or subject to further willful unauthorized disclosure.
    - A covered entity is deemed in compliance with the Arizona statute if it maintains and complies with its own notification requirements as part of an information security policy that are consistent with the Arizona statute is deemed in compliance, or it complies with notification requirements or procedures imposed by its primary or functional state or federal regulator.

- **Civil penalties:**
  - Actual damages for a willful and knowing violation of the statute.
  - Civil penalty not to exceed $10,000 per affected individual or the total amount of economic loss sustained by affected individuals, with a maximum civil penalty from a breach or series of related breaches of $500,000.

**Exemptions:**

- **Privacy Act of 1974:**
  - Entities subject to the GLBA are exempt.
  - Entities covered by the Health Insurance Portability and Accountability Act (“HIPAA”) are exempt.

**Other Obligations:**

- **Return to Index of States**
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arkansas</td>
<td>Information Covered: Personal information of Arkansas residents. Definition includes medical information. Important definitions: “Security Breach” means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a person or business. “Medical Information” means any individually identifiable information regarding medical history or medical treatment or diagnosis by a health care professional.</td>
<td>Subject to statute: Any person or business that acquires, owns or licenses computerized data that includes personal information about Arkansas residents.</td>
<td>Written or electronic notice must be provided to victims of a security breach within the most expedient time and manner possible and without unreasonable delay, unless a law enforcement agency determines that such notification will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td>Violations are punishable under the provisions of the state deceptive trade practices laws (Ark. Code 4-88-101 et seq.).</td>
<td>Private Cause of Action: No.</td>
</tr>
<tr>
<td>Arkansas</td>
<td>Third party recipients: Person or business maintaining (but not owning) computerized data that includes personal information must notify owner or licensee of data of any security breach immediately following discovery of security breach.</td>
<td>Other obligations: Data destruction or encryption mandatory when records with personal information are to be discarded. Covered entities must implement and maintain reasonable security procedures and practices to protect personal information.</td>
<td>A waiver of the statute is void and unenforceable.</td>
<td>Other exemptions: Exemption for good faith acquisition by an employee or agent of a covered entity for a legitimate purpose so long as personal information not otherwise used or subject to further unauthorized disclosure. Entities regulated by any state or federal law that provides greater protection to personal information and similar disclosure requirements are exempt.</td>
<td></td>
<td>Enforcement by Attorney General only.</td>
<td></td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties / Private Cause of Action / Enforcement</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>California</td>
<td>Personal information of California residents.</td>
<td>Any person or business that conducts business in California and owns or licenses computerized data that includes personal information.</td>
<td>Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines notification will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).</td>
<td>Encryption Safe Harbor: A breach of encrypted data triggers a notification requirement if the encryption key or security credential is also acquired by an unauthorized person, and the owner or licensor of the affected data reasonably believes that the encryption key or security credential could be used to render the encrypted personal information readable or usable.</td>
<td>Notification to the California Attorney General must be notified if a single breach results in notification to more than 500 California residents.</td>
<td>Civil remedies available to customers injured by a violation of the statute.</td>
<td></td>
</tr>
</tbody>
</table>

**California has specific statutes which could apply if medical information is compromised.**

**Important Definitions:**

- "Security Breach" means an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a covered entity.
- "Note (eff. 1/1/2017): A covered entity shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted personal information readable or usable. **A waiver of the statute is void and unenforceable.**
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>California, cont’d</td>
<td>Information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable</td>
<td>“Medical Information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.</td>
<td>“Medical Information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.</td>
<td>Encrypted means rendered unusable, unreadable or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.</td>
<td>Notice provided in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question and answer (or take other steps to protect online account).</td>
<td>Private Cause of Action (See Cal. Civ Code 1798.81):</td>
<td>for Economic and Clinical Health Act (“HITECH”).</td>
</tr>
</tbody>
</table>

**Return to Index of States**
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colorado</td>
<td>Information covered: Personal information of Colorado residents.</td>
<td>Subject to statute: Individual or commercial entity that conducts business in Colorado and owns or licenses computerized data that includes personal information.</td>
<td>Written, electronic or telephonic notice must be provided to victims as soon as possible following an investigation initiated promptly after determining it is likely personal information has been or will be misused. Notice must be made in the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted, redacted or secured by any other method rendering it unreadable or unusable.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td>Attorney General may bring actions in law or equity to seek relief, including direct economic damages resulting from a violation.</td>
<td>Private Cause of Action: No. Enforcement by Attorney General only</td>
</tr>
<tr>
<td>Click here to review text of statute (see Col. Rev. Stat. Title 6, Article 1, §6-1-716).</td>
<td>Important definitions: “Security Breach” means an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of the personal information.</td>
<td>Third party recipients: If covered entity maintains computerized data including personal information that the covered entity does not own or license, the covered entity must give notice to and cooperate with the owner or licensee of the information of any breach immediately following discovery if misuse of personal information is likely to occur.</td>
<td>Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 250,000 persons, or covered entity has insufficient contact information. Notice not required if investigation determines that the misuse of information about a resident has not occurred and is not reasonably likely to occur.</td>
<td>Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of covered entity so long as personal information not used or subject to further unauthorized disclosure. Entities regulated by state or federal law that maintain and comply with procedures for addressing security breaches pursuant to those laws are exempt.</td>
<td>Other obligations: Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.</td>
<td>Any covered entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with timing requirements of statute is deemed to be in compliance with Colorado statute.</td>
<td>Return to Index of States</td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------------------------------------</td>
<td>----------------------------------</td>
<td>----------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Connecticut</td>
<td>Information covered: Personal information of Connecticut residents.</td>
<td>Subject to statute: Any person who conducts business in Connecticut, and who, in the ordinary course of such person's business, owns licenses or maintains computerized data that includes personal information.</td>
<td>Written, electronic or telephonic notice must be provided within ninety (90) days to victims of a security breach without unreasonable delay following an investigation, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).  • Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.  • Notice not required if the entity responsible for the data determines in consultation with federal, state and local law enforcement that there is no reasonable likelihood of harm to individuals whose information has been acquired and accessed.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is secured by encryption or by any other method or technology that renders it unreadable or unusable.</td>
<td>Attorney General must be notified not later than time notice is provided to residents.  A determination of no likelihood of harm: Must be made in consultation with federal, state or local law enforcement.</td>
<td>Failure to comply with statute constitutes an unfair trade practice.</td>
<td>Private Cause of Action: No.  Enforcement by Attorney General only.</td>
</tr>
<tr>
<td></td>
<td>Important definitions: “Security Breach” means unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.</td>
<td>Third party recipients: If a covered entity maintains computerized data that includes personal information that the entity does not own, the entity must notify the owner or licensee of the information of any security breach immediately following discovery if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Click here to review text of statute (See Conn. Gen. Stat. §36a-701b).] [For specific rules applicable to state agencies and contractors providing goods and services to a state agency – click here.]
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delaware</td>
<td>This amended statute may go into effect as early as March 14, 2018. The legislation as signed by Delaware’s governor establishes an effective date 240 days after enactment, or April 14, 2018; however, the revised statute as published at Delaware Code Online indicates that the amendment goes into effect on March 14, 2018.</td>
<td>Delaware resident. Definition includes (i) passport number or other federal identification card number; (ii) a username or email address combined with a security question and answer or password that would grant access to a resident’s online account; (iii) medical history, medical treatment by a healthcare professional, diagnosis of any medical (mental or physical) condition by a healthcare professional, or DNA profile; (iv) health insurance subscriber identification number or any other health insurance unique identifier; (v) individual biometric information generated from assessment of human body characteristics for authentication purposes; and (vi) taxpayer identification number.</td>
<td>Written, telephonic or electronic notice must be provided to victims of a security breach as soon as possible following an appropriate investigation to determine if personal information has been or is reasonably likely to be misused. Notice must be made without unreasonable delay but no later than sixty (60) days following the discovery of the breach, unless a shorter time is required by federal law, or a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). Substituting notice is available by means prescribed in the statute if costs to exceed $75,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. If a resident’s Social Security number was compromised in the breach, complimentary credit monitoring services must be offered to the resident for one year; notice may not be given by e-mail to a resident whose related online account has been compromised. Notice not required if, after an appropriate investigation, the entity responsible for the personal information determines that the breach of security is unlikely to result in harm to individuals whose personal information has been breached.</td>
<td>Statute not applicable if personal information subject to a security breach is encrypted, unless an unauthorized acquisition includes, or is reasonably believed to include, an encryption key that could render the personal information readable or useable. Delaware Attorney General must be notified if a breach involves over 500 residents. A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td>Delaware Attorney General may bring actions in law or equity to seek appropriate relief, including direct economic damages resulting from a violation.</td>
<td>Attorney General may bring actions in law or equity to seek appropriate relief, including direct economic damages resulting from a violation.</td>
<td></td>
</tr>
</tbody>
</table>

Other exemptions, cont’d: A covered entity is deemed in compliance with the Delaware statute if it is regulated by state or federal law, including HIPAA and GLBA, and it complies with requirements or procedures imposed by its primary or functional state or federal regulator which are consistent with the Delaware statute.

A determination of no likelihood of harm: Does not require notification to Attorney General. | | Attorney General may bring actions in law or equity to seek appropriate relief, including direct economic damages resulting from a violation. |

Other exemptions, cont’d: A covered entity is deemed in compliance with the Delaware statute if it is regulated by state or federal law, including HIPAA and GLBA, and it complies with requirements or procedures imposed by its primary or functional state or federal regulator which are consistent with the Delaware statute.

A determination of no likelihood of harm: Does not require notification to Attorney General. | | Attorney General may bring actions in law or equity to seek appropriate relief, including direct economic damages resulting from a violation. |
### Florida

**Click here to review text of statute.**

<table>
<thead>
<tr>
<th>Information covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
</table>
| **Information covered:**

- Personal information of Florida residents.
- Definition includes (i) medical history, (ii) mental or physical condition, (iii) medical treatment or diagnosis by a health care professional, (iv) health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual, and (v) a user name or e-mail address in combination with a password or security question and answer that would permit access to the account.

**Important definitions:**

- "Security Breach" means unauthorized access of data in electronic form containing personal information.

| Subject to statute: Any legal or commercial entity that acquires, maintains, stores or uses personal information. (Definition also includes government entities in some instances.)
| Third party recipients: In the event of a security breach of a system maintained by a third party agent, such third party agent must cooperate with and notify the covered entity as expeditiously as practicable but not later than ten (10) days following determination of the breach.

| Written or electronic notice must be provided to Florida residents whose personal information was, or is reasonably believed to have been, accessed as a result of a security breach as expeditiously as practicable but not later than thirty (30) days following the determination of the breach. The notification may be delayed upon the written request of law enforcement.  
- Specific content requirements prescribed by statute for notice to individuals.
- Substitute notice is available by means described in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.
- Notice not required if the entity responsible for the data concludes after a reasonable investigation and consultation with federal, state and local law enforcement agencies 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.

| Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, secured or modified to remove elements that personally identify an individual or otherwise render the information unusable.

| Other exemptions:

- Exemption for good faith acquisition of personal information by an employee or agent of covered entity so long as personal information is not used for purposes unrelated to the business or subject to further unauthorized use.

- Entities notifying individuals in compliance with requirements of primary or functional federal regulator are deemed in compliance with Florida requirements provided notice is timely provided to Florida Department of Legal Affairs.

| Florida Department of Legal Affairs must be notified not later than thirty (30) days after determination of breach if more than 500 Florida residents are affected. Additional notification time may be obtained by request to the Florida Department of Legal Affairs within the 30 day period.

| Specific content requirements prescribed in statute for notification to Department of Legal Affairs.

| A determination of no likelihood of harm: Must be made in consultation with relevant federal, state or local law enforcement agencies. Such a determination must be documented in writing and maintained for at least 5 years. Covered entity must provide the written determination to the Florida Department of Legal Affairs within 30 days of determination.

| Violations are treated as an unfair or deceptive trade practice. For failure to provide notice of the security breach within 30 days: (i) $1,000 per day for first 30 days following violation, then (ii) up to $50,000 for each subsequent 30-day period up to 180 days, then (iii) an amount not to exceed $500,000 if violation continues. Penalties apply per breach, not per affected individual. Penalties do not apply to government entities. |

**Key Terms:**

- "Security Breach" refers to unauthorized access of data in electronic form containing personal information.
- "Written or electronic notice" must be provided to Florida residents whose personal information was accessed as a result of a security breach.
- "Encryption Safe Harbor" applies if personal data is encrypted, secured, or modified to remove personally identifying elements.
- "Other exemptions" cover certain circumstances, such as good faith acquisition.

**Legal Notes:**

- The statute outlines specific requirements for notice and encryption practices.
- Violations are subject to penalties, including daily fines and potential additional fees.

**Retrieved from:** Mintz Levin Cohn Ferris Glovsky & Popeo, P.C. and Florida Department of Legal Affairs.
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Georgia</td>
<td>Click here to review text of statute (see Ga. Code Ann., Title 10, Chapter 1, §910 et seq.)</td>
<td></td>
<td>Written, telephonic or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). Substitute notice is available by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of covered entity so long as personal information not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Georgia statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Georgia statute.</td>
<td></td>
<td>A state agency that has been subject to a certain single breach or aggravated computer tampering to the security of its data shall submit a comprehensive report to the attorney general and the General Assembly, specifies the content of the report, requires the report to be made available to the public.</td>
<td>Private Cause of Action: No.</td>
</tr>
</tbody>
</table>

Information covered: Personal information of Georgia residents. Definition includes any data elements when not in connection with a victim's first or last name if data element would be sufficient to allow someone to perform or attempt to perform identity theft.

Important definitions:

“Security Breach” means an unauthorized acquisition of an individual’s electronic data that compromises the security, confidentiality or integrity of personal information.

“Information Broker” means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties.

Subject to statute:

Any information broker that maintains computerized data that includes personal information.

Third party recipients:

Any person or business that maintains computerized data on behalf of covered entity that includes personal information that the person or business does not own must notify the covered entity who owns the information of any security breach within 24 hours following discovery of the breach.

Written, telephonic or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). Substitute notice is available by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information.

Other obligations:

Any information broker that must notify more than 10,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hawaii</td>
<td>Information covered: Personal information of Hawaii residents. Important definitions: “Security Breach” means an incident or unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and 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 or key constitutes a security breach. “Encryption” means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. “Redacted” means the rendering of data so that it is unreadable or truncated so that no more than the last four digits of the identification number are accessible as part of the data.</td>
<td>Subject to statute: Any business that owns or licenses personal information of residents, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes. Third party recipients: Any business located in Hawaii or that conducts business in Hawaii that maintains or possesses records or data with personal information of residents that the business does not own or license must notify the owner or licensee of any security breach immediately following discovery of the breach consistent with law enforcement needs.</td>
<td>Written, telephonic or electronic notice must be provided to victims of a security breach without unreasonable delay, unless law enforcement determines that disclosure could impede a criminal investigation or jeopardize national security (in which case notification is delayed until authorized by law enforcement). Specific requirements for the form and content of notice are described in the statute. Substitute notice is available by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 200,000 persons, or covered entity does not have sufficient contact information. Notice not required if the covered entity determines that it is not reasonably likely that illegal use of the personal information has or will occur or it is not reasonably likely that the security breach creates a risk of harm to a person. Other obligations: If more than 1,000 persons are notified at one time under the Hawaii statute, notification must also be made to applicable consumer reporting agencies.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted and the confidential process or key is not also compromised. Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of covered entity so long as personal information not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure. Certain financial institutes subject to federal regulations are exempt.</td>
<td>Hawaii Office of Consumer Protection must be notified if a breach involves over 1000 residents. A determination of no likelihood of harm: Does not require notification to Attorney General. A waiver of the statute is void and unenforceable.</td>
<td>Penalties not to exceed $2,500 per violation. Violators may also be liable to injured parties for actual damages sustained as a result of the violation. Reasonable attorney fees may also be awarded to the prevailing party.</td>
<td>Private Cause of Action: No. Enforcement by the Attorney General or executive director of the office of consumer protection.</td>
</tr>
</tbody>
</table>

Return to Index of States
Idaho

Information covered:
Personal information of Idaho residents.

Important definitions:
“Security Breach” means an illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality or integrity of personal information for one or more persons.

“Primary Regulator” of a commercial entity or individual licensed or chartered by the United States is that commercial entity's or individual's primary federal regulator. The primary regulator of a commercial entity or individual licensed by the department of finance is the department of insurance. The primary regulator of a commercial entity or individual licensed by the department of finance is the department of insurance. The primary regulator of a commercial entity or individual licensed by the department of finance is the department of insurance. The primary regulator of a commercial entity or individual licensed by the department of finance is the department of insurance. The primary regulator of a commercial entity or individual licensed by the department of finance is the department of insurance.

Subject to statute:
An individual, state, or a commercial entity that conducts business in Idaho and owns or licenses computerized data that includes personal information about a resident of Idaho.

Third party recipients:
Any covered entity that maintains computerized data that includes personal information that the covered entity does not own or license must give notice to and cooperate with the owner or licensee of the information of any security breach concerning the personal information of an Idaho resident.

Written, electronic or telephonic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay following a prompt investigation to determine if misuse of information about an Idaho resident has occurred or is reasonably likely to occur, unless a law enforcement agency determines that notice will impede a law enforcement investigation (in which case notification is delayed until authorized by law enforcement).

Substitute notice is available by means prescribed in the statute if costs to exceed $25,000, affected class exceeds 50,000 persons, or covered entity does not have sufficient contact information.

Notice only required if security breach materially compromises the security, confidentiality or integrity of personal information.

Notice not required if, after a reasonable and prompt investigation, the covered entity determines that there is no reasonable likelihood that personal information has been or will be misused.

Encryption Safe Harbor:
Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted.

Other exemptions:
Exemption for good faith acquisition by an employee or agent of the covered entity so long as personal information not used or subject to unauthorized disclosure.

A covered entity is deemed in compliance with the Idaho statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Idaho statute.

Entities regulated by state or federal law that maintain and comply with procedures for addressing security breaches pursuant to those laws are exempt.

A determination of no likelihood of harm:
Does not require notification to Attorney General if covered entity is an individual or commercial entity.

Notification to Regulator / Waiver:
Fine of not more than twenty-five thousand dollars ($25,000) per security breach for any covered entity that intentionally fails to give notice.

Any governmental employee that intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor and, upon conviction thereof, could be punished by a fine of not more than $2,000, or by imprisonment in the county jail for a period of not more than one year, or both.

Private Cause of Action: No.

Encryption Safe Harbor / Other Exemptions:
Covered Entities / Third Party Recipients:

Information Covered / Important Definitions:

Penalties:

Private Cause of Action / Enforcement:

State / Link to Statute

Information Covered / Important Definitions

Covered Entities / Third Party Recipients

Notice Procedures & Timing / Other Obligations

Encryption Safe Harbor / Other Exemptions

Notification to Regulator / Waiver

Penalties

Private Cause of Action / Enforcement

Return to Index of States

Copyright © 2009-2018 Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.
Current as of June 1, 2018 – FOR INFORMATIONAL PURPOSES ONLY

Boston | London | Los Angeles | New York | San Diego | San Francisco | Washington mintz.com
Illinois

Click here to review text of statute.

Important definitions, cont’d

"Health insurance information" means 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.

Return to Index of States

State / Link to Statute | Information Covered / Important Definitions | Covered Entities / Third Party Recipients | Notice Procedures & Timing / Other Obligations | Encryption Safe Harbor / Other Exemptions | Notification to Regulator / Waiver | Penalties | Private Cause of Action / Enforcement
---|---|---|---|---|---|---|---
Illinois | Personal information of Illinois residents. Definition to include (i) medical information, (ii) health insurance information, (iii) unique biometric data generated from measurements or technical analysis of human body characteristics used by the covered entity to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data, and (iv) 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 unread or otherwise read the data elements have not been obtained through the security breach. | Any covered entity that maintains computerized data that includes personal information that the covered entity does not own or license must give notice to and cooperate with the owner or licensee of the personal information. Illinois may take the position that any unauthorized acquisition or use by a third party triggers the notification obligation regardless of materiality/ownership of the data. | Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay. Notification may be delayed if law enforcement agency determines notification will interfere with a criminal investigation and such agency provides the covered entity with a written request. | Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is fully encrypted or redacted. Safe harbor will not be applicable if the keys to unencrypt or unredact or otherwise read the personal information have also been acquired without authorization. | A determination of no likelihood of harm: Does not require notification to Attorney General. A waiver of the statute is void and unenforceable. | A violation of the statute constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. | A determination of no likelihood of harm: Does not require notification to Attorney General. A waiver of the statute is void and unenforceable. |
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indiana</td>
<td><a href="#">Click here to review text of statute (see Ind. Code, Title 24, §§ 24-4.9 et seq.)</a></td>
<td><a href="#">For specific rules applicable to state agencies – see Ind. Code Title 4, §§ 4-1-11 et seq.</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information covered:</td>
<td></td>
<td>Written, electronic, telephonic or facsimile notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency or the Attorney General determines that notice will impede a civil criminal investigation or jeopardize national security. Notification must occur as soon as possible after delay is no longer necessary or authorized by Attorney General or law enforcement agency.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted.</td>
<td>Attorney General must be notified of any security breach using a designated form.</td>
<td>Violations are actionable deceptive acts.</td>
<td>For violations of the notification rules: The Attorney General may bring an action to enjoin future violations of the statute, a civil penalty of not more than $150,000 per deceptive act, and the Attorney General's reasonable costs.</td>
</tr>
<tr>
<td></td>
<td>Personal information of Indiana residents.</td>
<td></td>
<td>Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity does not have sufficient contact information.</td>
<td>Safe harbor not available if encryption key has been compromised.</td>
<td>Click here for form.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Definition includes an unencrypted or unredacted Social Security Number standing alone.</td>
<td></td>
<td>Notice only required if the covered entity knows, should know, or has known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft or fraud affecting the Indiana resident.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Important definitions:</td>
<td></td>
<td>Other obligations: Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies. Covered entity must implement and maintain reasonable procedures to protect and safeguard personal information of Indiana residents. Covered entity must dispose of records or documents containing unencrypted or unredacted personal information by shredding, incinerating, mutilating, erasing or otherwise rendering personal information illegible or unusable.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>“Security Breach” means an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. Definition includes the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm or a similar media, even if the transferred data are no longer in a computerized format. Unauthorized acquisition of an encrypted portable electronic device on which personal information is stored is not a security breach if the encryption key has not been compromised.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>“Encrypted” means data that have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or data which are secured by another method that renders data unreadable or unusable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>“Redacted” means data have been altered or truncated so that no more than last four digits are accessible (or last five digits for social security numbers).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Return to Index of States</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------------------------------------</td>
<td>---------------------------------</td>
<td>---------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Iowa</td>
<td>Click here to review text of statute.</td>
<td>Subject to statute: Any person or legal business entity that owns or licenses computerized data that includes a consumer's personal information that is used in the course of business, vocation, occupation or volunteer activities.</td>
<td>Written or electronic notice must be given to any consumer whose personal information was included in the information that was breached in the most expeditious manner possible and without unreasonable delay, unless a law enforcement agency determines that notification will impede a criminal investigation and the agency has made a written request that the notification be delayed (in which case notification is delayed until authorized by law enforcement).</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was breached was encrypted, redacted or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable and the keys to unencrypt, unredact or otherwise read the data elements have not been compromised.</td>
<td>Director of Consumer Protection Division of Attorney General must be notified within five (5) business days if giving notice of a security breach to more than 500 residents.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General for individuals or commercial entities.</td>
<td>Violation is an unlawful practice.</td>
</tr>
<tr>
<td>Return to Index of States</td>
<td>Information covered: Personal information of Iowa residents.</td>
<td>Third party recipients: Any covered entity who maintains or otherwise possesses personal information on behalf of another covered entity must notify the owner or licensor of the information of any security breach of a consumer’s personal information immediately following discovery of security breach.</td>
<td>Notification procedures: (i) if the data was acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.</td>
<td>Other exemptions: Exemption for good faith acquisition of personal information by an employee of a covered entity for purposes of the covered entity so long as personal information is not used in violation of applicable law or in a manner that harms or poses a threat to the affected resident.</td>
<td>Director of Consumer Protection Division of Attorney General or commercial entities.</td>
<td>Penalties for violation.</td>
<td>Private Cause of Action: No.</td>
</tr>
</tbody>
</table>

Important definitions:
- "Security Breach" means unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the personal information.
- Definition includes information maintained in any medium, including on paper, that was transferred by the person to that medium from computerized form.
- "Encryption" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.
- "Redacted" means altered or truncated so that no more than five digits of a social security number or the last four digits of other sensitive numbers are accessible.
### Kansas

**Information covered:** Personal information of Kansas residents.

**Definition:** Includes financial account number or credit card/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.

**Important definitions:**
- “Security breach” means unauthorized access to and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information and that causes, or the covered entity reasonably believes has caused or will cause, identity theft to any consumer.
- “Encrypted” means transformation of data through the use of algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable.
- “Redacted” means the alteration or truncation of data so that no more than five digits of a social security number, or the last four digits of a driver’s license number, state identification number or account number are accessible as part of the personal information.

**Subject to statute:** A person or legal entity that conducts business in Kansas that owns or licenses computerized data that includes personal information.

**Third party recipients:** An individual or commercial entity that maintains or otherwise possesses personal information that the individual or commercial entity does not own must notify the owner or licensee of the information of any security breach following discovery of unauthorized access and acquisition of personal information.

**Notice procedures & timing/other obligations:**
- Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).
  - Substitute notice is available by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 5,000 persons, or covered entity does not have sufficient contact information.
  - Notification is not required if, after a reasonable and prompt investigation, the covered entity determines it is not reasonably likely that misuse of the personal information has or will occur.

**Encryption safe harbor/other exemptions:**
- Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted.
- Other exemptions: Kansas statute does not apply to an individual or commercial entity that complies with notification requirements imposed by its primary or functional federal regulator.

**Other obligations:**
- Any person that must notify more than 1,000 persons at one time of a security breach is also required promptly to notify consumer reporting agencies.
- A covered entity must take reasonable steps to destroy or arrange for destruction of customer’s records within its custody or control containing personal information by shredding, erasing or otherwise modifying personal information so it is no longer readable or decipherable.

**Notification to regulator/waiver:**
- A determination of no likelihood of harm: Does not require notification to Attorney General.
- Other exemptions: Kansas statute does not apply to an individual or commercial entity that maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Kansas statute.

**Penalties:**
- Attorney General empowered to bring actions in law or equity to address violations.
- The Kansas insurance commissioner has sole authority over insurance companies who violate the Kansas statute.

**Private cause of action/enforcement:** Private Cause of Action: No.
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kentucky</td>
<td>Information covered: Kentucky residents. [For specific rules applicable to government agencies - click here.]</td>
<td>Subject to statute: <code>Any person or business entity that conducts business in Kentucky. Also covered are NTP’s per KRS §61.931.</code></td>
<td>Written or electronic notice must be provided to victims of a security breach in the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).  • <strong>Substitute notice is available</strong> by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity does not have sufficient contact information.  • <strong>Notice only required</strong> by a security breach that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.</td>
<td>[An NTP must notify its contracting agency or institution within 72 hours of determining that a breach occurred. The contracting agency or institution is responsible for notifying affected individuals.]</td>
<td>Attorney General may seek equitable and/or legal remedies.</td>
<td>Private Cause of Action: No.</td>
</tr>
<tr>
<td>Kentucky</td>
<td>Important definitions: Security Breach means unauthorized acquisition of unencrypted and unreconstructed computerized data that compromises the security, confidentiality or integrity of personal information maintained by the covered entity as part of a database regarding multiple individuals that actually causes, or leads the covered entity to reasonably believe has caused or will cause, identify theft or fraud against a Kentucky resident. Nonaffiliated Third Party (NTP) means any person that has a contract or agreement with (and receives personal information from) a government agency, subdivision, instrumentality or unit, including such institutions as a public school or public institute.</td>
<td><strong>Third party recipients:</strong> A covered entity that maintains or otherwise possesses personal information that the individual or commercial entity does not own must notify the owner or licensee of the information of any security breach as soon as reasonably practicable following discovery of security breach.</td>
<td>Other obligations: A covered entity that must notify more than 1,000 consumers at one time of a security breach is also required to promptly notify all consumer reporting agencies of the security breach. A business disposing of customer records must take reasonable steps to destroy the records with personal information by shredding, erasing or otherwise modifying the personal information to make it unreadable or indecipherable.</td>
<td>Other exemptions: Exemption for good faith acquisition by an employee or agent of the covered entity for the purposes of the covered entity, so long as personal information is not used or subject to further unauthorized disclosure.</td>
<td>Does not require notification to Attorney General.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td></td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>PrivateCause of Action / Enforcement</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------</td>
<td>-----------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Louisiana</td>
<td>Information covered: Personal information of Louisiana residents.</td>
<td>Subject to statute: Any person or legal entity that conducts business in Louisiana or that owns or licenses computerized data that includes personal information.</td>
<td>Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted.</td>
<td>Consumer Protection Section of Attorney General must be notified of a security breach within ten (10) days of distribution of notice to affected Louisiana citizens. Consumer Protection Section of Attorney General must be notified of a security breach within ten (10) days of distribution of notice to affected Louisiana citizens.</td>
<td>Civil action may be instituted to recover actual damages.</td>
<td>Yes.</td>
</tr>
<tr>
<td></td>
<td>Important definitions: “Security Breach” means 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.</td>
<td>Third party recipients: Any covered entity that maintains computerized data that includes personal information that the covered entity does not own must notify the owner or licensee of the information following discovery of a security breach.</td>
<td>Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity does not have sufficient contact information.</td>
<td>Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of the covered entity for the purposes of the covered entity, so long as personal information is not used or subject to further unauthorized disclosure.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td>Failure to provide timely notice punishable by a fine not to exceed $5,000 per violation. Notice to state Attorney General will be &quot;timely&quot; if received within ten (10) days of distribution of notice to Louisiana citizens. Each day notice is not received by Attorney General is deemed a separate violation.</td>
<td></td>
</tr>
</tbody>
</table>

Return to Index of States

Click here to review text of statute.

Click here to review additional rules (see La. Admin. Code, Title 16, § 701)
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
</table>
| Maine                  | Information covered: Personal information of Maine residents. Data elements alone are considered personal information if the data would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. Definition does not include 3rd party claims databases maintained by property and casualty insurers. Important definitions: “Security Breach” means unauthorized acquisition, release or use of an individual’s computerized data that contains personal information that compromises the security, confidentiality or integrity of the personal information. “Encryption” means the disguising of data using generally accepted practices. “Information Broker” means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties. | Subject to statute: Any information broker, individual, legal entity and private colleges and universities that maintain computerized data that includes personal information. Third party recipients: Any third party entity that maintains, on behalf of a covered entity, computerized data that includes personal information that the third party does not own must notify the owner following discovery of a security breach. | Written or electronic notice must be provided to victims of a security breach as expeditiously as possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification may be delayed for no longer than seven (7) business days after a law enforcement agency authorizes the notification).  
- Substitute notice is available by means prescribed in the statute if costs to exceed $5,000, affected class exceeds 1,000 persons, or covered entity does not have sufficient contact information.  
- Notice not required if, after a reasonable and prompt investigation, the covered entity determines that there is no reasonable likelihood that personal information has been or will be misused. | Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Other exemptions: Exemption for good faith acquisition, release or use of personal information by employee or agent acting on behalf of covered entity so long as personal information is not used for or subject to further unauthorized disclosure. Covered entity deemed in compliance with the statute if it complies with other federal or state security breach notification requirements at least as protective as Maine statute. | Attorney General or Department of Professional and Financial Regulation must be notified of a security breach. Information brokers must notify the Department of Professional and Financial Regulation and all other covered entities must notify the Attorney General. A determination of no likelihood of harm: Does not require notification to Attorney General. | Fines of not more than $500 per violation, up to a maximum of $2500 per each day covered entity is in violation of statute. Equitable relief and enjoinment from future violations are also available. | The statute is enforced by the Department of Professional and Financial Regulation as to licensed data brokers and by the Attorney General as to all others. |
<table>
<thead>
<tr>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maryland</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Click here to review text of statute (see Md. Code Com. Law, Title 14, §§ 14-3501 et seq.)</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td><strong>Information covered:</strong></td>
<td><strong>Subject to statute:</strong></td>
<td><strong>Written, electronic or telephonic notice must be provided</strong></td>
<td><strong>Encryption Safe Harbor:</strong></td>
<td><strong>Notification to Regulator:</strong></td>
<td><strong>Penalties</strong></td>
<td><strong>Private Cause of Action:</strong></td>
</tr>
<tr>
<td>Personal information of Maryland residents</td>
<td>Any business that owns or licenses personal information of an individual residing in Maryland.</td>
<td>to victims of a security breach as soon as reasonably practicable after the business discovers or is notified of the breach of the security of a system, unless a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement agency).</td>
<td>Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted.</td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td><strong>Definition includes:</strong></td>
<td><strong>Third party recipients:</strong></td>
<td><strong>Specific requirements for the content of the notice are detailed in statute:</strong></td>
<td><strong>Other exemptions:</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>• Individual Taxpayer Identification Number.</td>
<td>A business that maintains computerized data that includes personal information that the business does not own or license must notify the owner or licensee of the information of any security breach if it is likely that the breach has resulted or will result in misuse of personal information of a Maryland resident.</td>
<td><strong>Specific requirements for the content of the notice are detailed in statute:</strong></td>
<td><strong>Exemption for good faith acquisition of personal information by an employee or agent of a business for the purpose of the business so long as personal information is not used or subject to further unauthorized disclosure.</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>• Passport Number and other ID numbers issued by federal government.</td>
<td><strong>Notification not required if, after investigation, the business determines that misuse of the personal information has not occurred or is not reasonably likely to occur. Records of such determination must be maintained for three years.</strong></td>
<td><strong>Substitute notice is available by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 175,000 persons, or covered entity does not have sufficient contact information.</strong></td>
<td><strong>A determination of no likelihood of harm:</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>• State ID card numbers</td>
<td></td>
<td></td>
<td><strong>Does not require notification to Attorney General.</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>• Health information (any information created by an entity covered by HIPAA regarding an individual’s medical history, condition, treatment or diagnosis).</td>
<td></td>
<td></td>
<td>A waiver of the statute is void and unenforceable.</td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. StateGovt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>• A health insurance policy, certificate, number or health insurance subscribe number in combination with a unique ID that permits access to the information</td>
<td></td>
<td></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>• Biometric data</td>
<td></td>
<td></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>• User name or email address in combination with a password or security Q&amp;A</td>
<td></td>
<td></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td><strong>Important definitions:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>• &quot;Security Breach&quot; means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>• &quot;Encrypted&quot; means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>[For specific rules applicable to state and government agencies – see also Md. State Govt. Code, Title 10, §§ 10-1301 et seq.]</strong></td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------</td>
<td>---------------------------------------</td>
<td>----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Massachusetts Click here to review text of statute.</td>
<td>Personal information of Massachusetts residents. Definition includes financial account number or credit/debit card number with or without any required security or access code or password that would permit access to a resident’s financial account.</td>
<td>A person that maintains or stores but does not own or license data that includes personal information about a Massachusetts resident.</td>
<td>Written or electronic notice must be provided to victims of a security breach as soon as practicable and without unreasonable delay after the covered entity discovers or is notified of a security breach, unless a law enforcement agency determines that the notification will impede a criminal investigation and has notified the Attorney General in writing of such determination (in which case notification is delayed until authorized by law enforcement agency).</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted and the process or key that is capable of unlocking the data has not been compromised.</td>
<td>Other exemptions: Covered entity is deemed in compliance with the Massachusetts statute if it maintains and complies with procedures for responding to a breach of security pursuant to federal laws and regulations provided the covered entity notifies the Attorney General and the Director of the Office of Consumer Affairs and Business Regulation of the security breach as soon as practicable and without unreasonable delay following discovery of the security breach. Notice must describe the steps to be taken.</td>
<td>Attorney General may bring an action under Chapter 93A, the Commonwealth’s consumer protection statute.</td>
</tr>
<tr>
<td>Return to Index of States</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Important definitions:**
- **“Security Breach”** means unauthorized acquisition or unauthorized use of unencrypted data, or of encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a Massachusetts resident.

**“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.

**“Encrypted”** means the transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

**Written or electronic notice must be provided to victims of a security breach as soon as practicable and without unreasonable delay after the covered entity discovers or is notified of a security breach, unless a law enforcement agency determines that the notification will impede a criminal investigation and has notified the Attorney General in writing of such determination (in which case notification is delayed until authorized by law enforcement agency).**

- Notification must tell affected residents that a breach occurred but may not discuss the nature of the breach/unauthorized acquisition or the number of Massachusetts residents affected by the breach.
- Notification to affected residents required to contain specific content described in the statute.
- Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity does not have sufficient contact information.
- Notice only required after a security breach that causes substantial risk of identity theft or fraud or after a covered entity has reason to know that the personal information of a Massachusetts resident was acquired by an unauthorized person or used for an unauthorized purpose.

**Other obligations:**
- Paper records containing personal information must be redacted, burned, pulverized or shredded.
- Electronic data containing personal information must be destroyed or erased.

**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted and the process or key that is capable of unlocking the data has not been compromised. **Other exemptions:** Covered entity is deemed in compliance with the Massachusetts statute if it maintains and complies with procedures for responding to a breach of security pursuant to federal laws and regulations provided the covered entity notifies the Attorney General and the Director of the Office of Consumer Affairs and Business Regulation of the security breach as soon as practicable and without unreasonable delay following discovery of the security breach. Notice must describe the steps to be taken.

| Attorney General and Office of Consumer Affairs and Business Regulation (“OCABR”) must be separately notified of a security breach as soon as practicable after becoming aware of security breach. Notice to the OCABR must be submitted through an online portal – click here. Notice to regulators may be required even in cases where security breach involves encrypted data. Covered entity must be able to determine that the key or confidential process has not been compromised. The covered entity must also provide notice to any consumer reporting agencies and state agencies identified by the OCABR. **A determination of no likelihood of harm:** Does not require notification to Attorney General. |

**Penalties:**
- A civil penalty of $5,000 may be awarded for each violation (see 93A §4). Businesses can be subject to a fine of up to $50,000 for each instance of improper disposal of data (see 93I §2).
- If Attorney General finds violation of consumer protection laws for unfair or deceptive acts or practices, Massachusetts consumers may seek damages under Chapter 93A, which, in some cases, may be trebled.

**Note:** The OCABR has launched a web-based public archive of data breaches affecting Massachusetts residents: click here.
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Massachusetts, cont’d</td>
<td>Information covered: Personal information of Massachusetts residents. Definition includes financial account number or credit/debit card number with or without any required security or access code or password that would permit access to a resident’s financial account.</td>
<td>Subject to statute: Every person or legal entity that owns, licenses, stores or maintains personal information about a Massachusetts resident. Third party recipients: Covers third-party service providers with access to personal information.</td>
<td>The regulations require the development, implementation and maintenance of a comprehensive information security program consistent with industry standards and state or federal regulations applicable to the covered entity with respect to owning or licensing personal information. See 201 CMR 17.00 for a detailed description of content requirements and technology requirements for the comprehensive information security program. The sufficiency of a comprehensive information security program will be evaluated by taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information. Other obligations: Requires entities to collect and store the minimum amount of personal information necessary to accomplish the legitimate purpose for which it was collected, and requires entities to restrict access to the personal information to the smallest possible number of users.</td>
<td>Encryption Requirements: The regulations require the encryption of all transmitted records and files containing personal information, including those in wireless environments, which will travel across public networks. For files containing personal information on a system that is connected to the Internet, there must be firewall protection with up-to-date patches, including operating system security patches. Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the lawful purposes of the covered entity so long as personal information is not used in an unauthorized manner or subject to further unauthorized disclosure.</td>
<td></td>
<td></td>
<td>Please see above for a summary of applicable penalty provisions of Mass. Gen. Laws. c. 93A, c. 93H and c. 93I. Please see above. Consumers may seek damages under Mass. Gen. Laws. c. 93A.</td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------</td>
<td>---------------------------------</td>
<td>----------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Michigan</td>
<td>Information covered: Personal information of Michigan residents.</td>
<td>Subject to statute: Any person or legal entity that owns or licenses personal information that is included in a database.</td>
<td>Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay. Notification may be delayed if law enforcement agency determines that notification will impede a criminal or civil investigation or jeopardize homeland or national security. Notification must occur without unreasonable delay following authorization from the law enforcement agency.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted and the encryption key was not compromised.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General for individuals or commercial entities.</td>
<td>Civil penalty for failure to provide notice of not more than $250 for each failure to provide notice, capped at $750,000 per security breach.</td>
<td>Private Cause of Action: No.</td>
</tr>
<tr>
<td></td>
<td>Important definitions: “Security Breach” means unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a covered entity as part of a database of personal information regarding multiple individuals. “Encrypted” means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable. “Redact” means to alter or truncate data so that no more than four sequential digits of a driver license number, state personal identification card number, or account number, or no more than five sequential digits of a social security number, are accessible as part of personal information.</td>
<td>Third party recipients: A covered entity that maintains a database that includes data that the person does not own or license must notify the owner or licensor of the information of a security breach unless the covered entity determines that 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 Michigan residents</td>
<td>Notice to affected residents is required to contain specific content described in the statute.</td>
<td>Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity related to their activities for the covered entity so long as employee or agent does not misuse personal information or disclose any personal information to an unauthorized person. Financial institutions that are subject to and comply with notification procedures from an appropriate regulator are exempt from Michigan statute.</td>
<td>A waiver of the statute is void and unenforceable.</td>
<td>Criminal penalties for notice of a security breach that has not occurred, where such notice is given with the intent to defraud. Misdemeanor – 93 days imprisonment or fine of $250 (or both) for each violation (penalties escalate with more violations).</td>
<td></td>
</tr>
</tbody>
</table>

Other obligations: Any covered entity that must notify more than 1,000 residents at one time of a security breach is also required to notify consumer reporting agencies of the security breach without unreasonable delay (unless subject to GLBA).
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minnesota</td>
<td>Information covered: Personal information of Minnesota residents. Important definitions: &quot;Security Breach&quot; means an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. Definition does not include loss of a portable electronic device containing password protected personal information if the encryption key or process is not compromised.</td>
<td>Subject to statute: Any person or business doing business in Minnesota that owns or licenses computerized data containing personal information. Third party recipients: A covered entity that maintains data that includes personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach immediately following discovery.</td>
<td>Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted and the encryption key, password or other means necessary for reading or using the data has not been acquired.</td>
<td></td>
<td></td>
<td>Enforce under Minn. Stat. §8.31.</td>
</tr>
</tbody>
</table>

Return to Index of States
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
</table>
| Mississippi            | Information covered: Personal Information of a Mississippi resident. | Subject to statute: Any person who conducts business in Mississippi and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any Mississippi resident. | Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay following completion of an investigation, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).  
- Substitute notice by means prescribed in the statute if costs to exceed $5,000, affected class exceeds 5,000 persons, or covered entity has insufficient contact information.  
- Notice not required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals. | Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or otherwise rendered unreadable or unusable. | A determination of no likelihood of harm: Does not require notification to Attorney General. | Failure to comply is a violation of state’s unfair trade practice. | Private Cause of Action: No.  
Enforcement by Attorney General only. |

Mississippi Click here to review text of statute (see Miss. Code, Title 75, § 75-24-29).
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
</table>
| Missouri               | Information covered: Personal information of Missouri residents. Definition includes (i) unique electronic identifier or routing code in combination with required security code, access code, or password, (ii) medical information, or (iii) health insurance information. Important definitions: “Security Breach” means unauthorized access to and unauthorized acquisition of personal information maintained in a computerized form that compromises the security, confidentiality or integrity of the personal information. “Health Insurance Information” means an individual’s health insurance policy number or subscriber number or any unique identifier used by a health insurer to identify the individual. “Medical Information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. “Encryption” means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. “Redacted” means altered or truncated such that no more than five digits of a Social Security Number or the last four digits of a driver’s license number, state ID or account number is accessible. | Subject to statute: Any person or legal or commercial entity that conducts business in Missouri and that owns or licenses personal information of Missouri residents in any form. Third party recipients: Any person that maintains or possesses records or data containing personal information of Missouri residents that the person does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach consistent with the legitimate needs of law enforcement. | Written, electronic or telephone notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).  
- Notice to affected residents is required to contain specific content described in the statute.  
- Substitute notice is available by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 150,000 persons, or covered entity has insufficient contact information. Substitute notice may also be used for consumers who the covered entity knows to be affected but is not able to identify.  
- Notice not required if, after an appropriate investigation by the covered entity or after consultation with the relevant federal, state or local agencies responsible for law enforcement, the covered entity 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 must be documented in writing and retained for five years. | Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise rendered unreadable or unusable. Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for a legitimate purpose so long as personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information. Covered entity deemed in compliance with the Missouri statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with Missouri’s timing requirements. Any business that complies with the notification procedures imposed by its primary or functional federal or state regulator is deemed in compliance with the Missouri statute. | Attorney General must be notified if a single breach results in notification to more than 1,000 Missouri residents. The notice must describe timing, distribution and content of notice to residents. A determination of no likelihood of harm: Does not require notification to attorney general. | For willful and knowing violations, actual damages and/or civil penalties not to exceed $150,000 for each security breach. |

**Other Exemptions**

- Financial institutions are exempt if they are subject to and comply with federal interagency guidelines.
Information covered: Personal information of Montana residents. Definition includes medical record information, taxpayer identification number, or an identity protection personal identification number issued by the United States internal revenue service.

Important definitions:
"Security Breach" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information and causes or is reasonably believed to cause loss or injury to a person.

"Medical Record Information" means personal information that: (a) relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment; and (b) is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent or legal guardian.

"Redaction" means the alteration of personal information contained within data to make all or a significant part of the data unreadable. The term includes truncation, which means that no more than the last four digits of an identification number are accessible as part of the data.

Subsequent to a security breach, any person or business that conducts business in Montana and owns or licenses computerized data that includes personal information.

Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).

- Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.
- Notice not required if covered entity determines that security breach has not materially compromised the security, confidentiality or integrity of personal information and has not caused or is not reasonably likely to cause loss or injury to a person.

Other Obligations:
If the notice provided suggests or implies that a consumer can obtain a copy of their file from a credit reporting agency, the business must coordinate with the credit reporting agency regarding the timing, content and distribution of notice to the Montana consumer so long as personal information is not used or subject to further unauthorized disclosure. Covered entity deemed in compliance with the Montana statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Montana statute.

Penalties:
Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).

- Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.
- Notice not required if covered entity determines that security breach has not materially compromised the security, confidentiality or integrity of personal information and has not caused or is not reasonably likely to cause loss or injury to a person.

Other Obligations:
If the notice provided suggests or implies that a consumer can obtain a copy of their file from a credit reporting agency, the business must coordinate with the credit reporting agency regarding the timing, content and distribution of notice to the Montana consumer so long as the coordination does not unreasonable delay the notice to the affected individuals.

Penalties:
Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).

- Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.
- Notice not required if covered entity determines that security breach has not materially compromised the security, confidentiality or integrity of personal information and has not caused or is not reasonably likely to cause loss or injury to a person.

Other Obligations:
If the notice provided suggests or implies that a consumer can obtain a copy of their file from a credit reporting agency, the business must coordinate with the credit reporting agency regarding the timing, content and distribution of notice to the Montana consumer so long as the coordination does not unreasonable delay the notice to the affected individuals.

Penalties:
Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).

- Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.
- Notice not required if covered entity determines that security breach has not materially compromised the security, confidentiality or integrity of personal information and has not caused or is not reasonably likely to cause loss or injury to a person.

Other Obligations:
If the notice provided suggests or implies that a consumer can obtain a copy of their file from a credit reporting agency, the business must coordinate with the credit reporting agency regarding the timing, content and distribution of notice to the Montana consumer so long as the coordination does not unreasonable delay the notice to the affected individuals.

Penalties:
Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).

- Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.
- Notice not required if covered entity determines that security breach has not materially compromised the security, confidentiality or integrity of personal information and has not caused or is not reasonably likely to cause loss or injury to a person.

Other Obligations:
If the notice provided suggests or implies that a consumer can obtain a copy of their file from a credit reporting agency, the business must coordinate with the credit reporting agency regarding the timing, content and distribution of notice to the Montana consumer so long as the coordination does not unreasonable delay the notice to the affected individuals.

Penalties:
Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).

- Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.
- Notice not required if covered entity determines that security breach has not materially compromised the security, confidentiality or integrity of personal information and has not caused or is not reasonably likely to cause loss or injury to a person.

Other Obligations:
If the notice provided suggests or implies that a consumer can obtain a copy of their file from a credit reporting agency, the business must coordinate with the credit reporting agency regarding the timing, content and distribution of notice to the Montana consumer so long as the coordination does not unreasonable delay the notice to the affected individuals.

Penalties:
Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).

- Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.
- Notice not required if covered entity determines that security breach has not materially compromised the security, confidentiality or integrity of personal information and has not caused or is not reasonably likely to cause loss or injury to a person.

Other Obligations:
If the notice provided suggests or implies that a consumer can obtain a copy of their file from a credit reporting agency, the business must coordinate with the credit reporting agency regarding the timing, content and distribution of notice to the Montana consumer so long as the coordination does not unreasonable delay the notice to the affected individuals.
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nebraska</td>
<td>Information covered: Personal information of Nebraska residents. Definition includes: (i) unique electronic identification number or routing code in combination with any required security code, access code or password, (ii) unique biometric data, such as fingerprint, voice print, or retina or iris image, or other unique physical representation, and (iii) a user name or email address in combination with a password or security question and answer that permits access to an online account. Important definitions: “Security Breach” means an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information. “Redact” means altering or truncating data in a way that only the last four digits of a social security number, driver’s license number, state identification card or account number are accessible. “Encrypted” means converted by use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. Data is not considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the security breach.</td>
<td>Subject to statute: Individual or commercial entity that conducts business in Nebraska and that owns or licenses computerized data which includes personal information about a Nebraska resident. Third party recipients: Any individual or commercial entity that maintains computerized data containing personal information that the individual or commercial entity does not own must notify the owner or licensee of the information of any security breach when it becomes aware of such breach if use of personal information for an unauthorized purpose occurred or is reasonably likely to occur. Written, electronic or telephonic notice must be provided to victims of a security breach as soon as possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). • Substitute notice is available by means prescribed in the statute if costs to exceed $75,000, affected class exceeds 100,000 persons, covered entity has insufficient contact information, or if the covered entity has ten employees or fewer and demonstrates that the cost of providing notice will exceed $10,000. • Notice not required if, after a reasonable and prompt investigation, the covered entity determines there is no reasonable likelihood that the personal information has been or will be used for an unauthorized purpose.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data (name or data elements) that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise altered such that the name or data elements are unreadable. Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to search warrant, subpoena or court order is not a security breach. Covered entity that maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Nebraska statute is deemed in compliance.</td>
<td>Attorney General must be notified not later than time when notice is provided to affected residents.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General. A waiver of the statute is void and unenforceable. Other exemptions, cont’d: Any covered entity that complies with the procedures imposed by its primary or functional federal or state regulator is deemed in compliance with the Nebraska statute if it notifies affected residents and the Attorney General in accordance with the maintained procedures in the event of a security breach.</td>
<td>Direct economic damages for each affected Nebraska resident injured by a violation.</td>
<td>Private Cause of Action: No. Enforcement by Attorney General only.</td>
</tr>
</tbody>
</table>

Return to Index of States
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
</table>
| Nevada | [Click here to review text of statute.](#) | Information covered:  
Personal information of Nevada residents when the name and the data elements are not encrypted.  
Definition includes (i) medical identification number, (ii) health insurance identification number, and (iii) 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.  
Important definitions:  
“Security Breach” means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information. | Subject to statute:  
Any institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that handles, collects, disseminates or otherwise deals with nonpublic personal information.  
Third party recipients:  
Any covered entity that maintains computerized data containing personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach.  
Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).  
- Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.  
- Notice only required if security breach materially compromises the security, confidentiality or integrity of personal information.  
Other obligations:  
Any covered entity that must notify more than 1,000 residents at one time of a security breach is also required to notify consumer reporting agencies of the security breach without unreasonable delay.  
A business maintaining records which contain personal information concerning customers must take reasonable measures to protect records from unauthorized access and, when they are no longer needed, ensure the destruction of those records in accordance with the statute.  
Encryption Safe Harbor:  
Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted.  
Other exemptions:  
Exemption for good faith acquisition of personal information by an employee or agent of the covered entity for a legitimate purpose of the covered entity so long as the personal information is not used for a purpose unrelated to the covered entity or subject to further unauthorized disclosure.  
A determination of no likelihood of harm:  
Does not require notification to Attorney General.  
A waiver of the statute is void and unenforceable. | A covered entity that provides the notification required by the Nevada statute may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the covered entity. Damages and restitution relief are available. | Attorney General may bring an action against a covered entity to obtain a temporary or permanent injunction against violations. | [mintz.com](http://mintz.com) |
### New Hampshire

**Click here to review text of statute (see N.H. Rev. Stat. §359-C:19, et seq.).**

**Information covered:** Personal information of New Hampshire.

New Hampshire has specific statutes which could apply if an individual’s medical information is compromised.

**Important definitions:**
- "Security Breach" means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information.
- "Encrypted" means the transformation of data through the use of an algorithmic process into a form for which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements completely unreadable or unusable.

**Subject to statute:** Any person, business, legal entity or governmental entity that conducts business in New Hampshire and owns, maintains or licenses computerized data that includes personal information.

**Third party recipients:** Any covered entity that maintains computerized data containing personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach and provide cooperation as needed and required by statute.

**Notice procedures & timing:**
- Written, electronic or telephonic notice must be provided to victims of a security breach as soon as possible.
  - Notice to affected residents is required to contain specific content described in statute.
  - Substitute notice is available by means prescribed in the statute if costs to exceed $5,000, affected class exceeds 1,000 persons, or covered entity has insufficient contact information.
  - Notification is not required if it is determined that misuse of the information has not occurred and is not reasonably likely to occur.

**Other obligations:**
- Any covered entity that must notify more than 1,000 consumers at one time of a security breach is also required to notify consumer reporting agencies of the security breach without unreasonable delay.
- Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted.
- Data acquired in combination with the required key, security code, access code or password is not considered encrypted.
- Exemption for good faith acquisition of personal information by an employee or agent of a person for the purposes of the person’s business as long as personal information is not used or subject to further unauthorized disclosure.
- Any person engaged in trade or commerce subject to RSA 358-A:3, I must notify the regulator which has primary regulatory over such trade or commerce. All others notify must notify the Attorney General. Notice must include anticipated date of notice to individuals affected and the approximate number of individuals in the state who will be notified.

**Notification to regulator / waiver:**
- Attorney General or the primary regulator applicable to covered entity must be notified of a security breach. Any person engaged in trade or commerce subject to RSA 358-A:3. I must notify the regulator which has primary regulatory over such trade or commerce. All others notify must notify the Attorney General.
- Civil penalties up to $10,000 per violation when actions brought by the Attorney General (injunctive and restitution relief also available). Private citizens injured as a result of violation may bring an action for damages and for equitable relief, including an injunction. Recovery will be actual damages (or up to two to three times actual damages if violation was knowing and willful).
- A prevailing plaintiff may also be awarded costs and reasonable attorney’s fees.

**Encryption Safe Harbor / Other Exemptions:**
- Attorney General or the primary regulator applicable to covered entity must be notified of a security breach. Any person engaged in trade or commerce subject to RSA 358-A:3. I must notify the regulator which has primary regulatory over such trade or commerce. All others notify must notify the Attorney General.
- A waiver of the statute is void and unenforceable.

**Other exemptions:**
- Data acquired in combination with the required key, security code, access code or password is not considered encrypted.
- Exemption for good faith acquisition of personal information by an employee or agent of a person for the purposes of the person’s business as long as personal information is not used or subject to further unauthorized disclosure.
- Any person engaged in trade or commerce subject to RSA 358-A:3, I must notify the regulator which has primary regulatory over such trade or commerce. All others notify must notify the Attorney General. Notice must include anticipated date of notice to individuals affected and the approximate number of individuals in the state who will be notified.
- A determination of no likelihood of harm:
  - Does not require notification to Attorney General.

**Penalties:**
- Attorney General or the primary regulator applicable to covered entity must be notified of a security breach. Any person engaged in trade or commerce subject to RSA 358-A:3. I must notify the regulator which has primary regulatory over such trade or commerce. All others notify must notify the Attorney General.
- A waiver of the statute is void and unenforceable.

**Private cause of action / enforcement:**
- Attorney General and affected residents can enforce.
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Jersey</td>
<td>Click here to review text of statute (see N.J. Stat., Title 56, §56:8-161 et seq.)</td>
<td>Subject to statute: Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information.</td>
<td>Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement).</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or secured by any other method or technology that renders the personal information unreadable or unusable.</td>
<td>Division of State Police in the Department of Law and Public Safety must be notified prior to notification to customers.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td>Private Cause of Action: No.</td>
</tr>
<tr>
<td></td>
<td>Information covered: Personal information of New Jersey residents. Data disassociated from a first name or first initial and last name is personal information if the means to link the disassociated data were accessed and compromised.</td>
<td>Third party recipients: Any covered entity that maintains computerized records containing personal information on behalf of another business or public entity must notify such other business or public entity of any security breach.</td>
<td>Substitute notice by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.</td>
<td>Notice not required if the covered entity establishes that misuse of the information is not reasonably possible. Such determinations must be documented in writing and retained for five (5) years.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Important definitions: “Security Breach” means 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 of technology that renders the personal information unreadable or unusable.</td>
<td>Other obligations: Any covered entity that must notify more than 1,000 consumers at one time of a security breach is also required to notify consumer reporting agencies of the security breach without unreasonable delay.</td>
<td>Any business or public entity must destroy or arrange for destruction any customer records within its custody or control containing personal information which it no longer needs by shredding, erasing or otherwise modifying the personal information so that it is unreadable, indecipherable or nonreconstructable through generally available means.</td>
<td>Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of covered entity for a legitimate business purpose so long as personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Information covered: Personal information of New Jersey residents. Data disassociated from a first name or first initial and last name is personal information if the means to link the disassociated data were accessed and compromised.

Important definitions: “Security Breach” means 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 of technology that renders the personal information unreadable or unusable.
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Mexico</strong></td>
<td>Information covered: Personal information of New Mexico residents. Definition includes biometric data. Important definitions: &quot;Biometric Data&quot; means 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. &quot;Encrypted&quot; means rendered unusable, unreadable or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security. &quot;Security Breach&quot; means the unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person. &quot;Service Provider&quot; means any person that receives, stores, maintains, licenses, processes or otherwise is permitted access to personal identifying information through its provision of services directly to a person that is subject to regulation.</td>
<td>Subject to statute: Any person that owns or licenses computerized data that includes personal information.</td>
<td>Written or electronic notice must be provided to New Mexico residents whose personal information is reasonably believed to have been subject to a security breach in the most expedient time possible but not later than forty-five (45) days following the determination of the breach, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). Specific content requirements prescribed by statute for notiication to individuals. Substitute notice is available by means described in the statute if costs to exceed $100,000, affected class exceeds 50,000 persons, or covered entity has insufficient contact information. Notice not required if the covered entity responsible for the data concludes after a reasonable investigation that the security breach does not give rise to a significant risk of identity theft or fraud.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal information that was acquired by an unauthorized individual is encrypted. Safe harbor not available if the confidential process or key is compromised together with the encrypted data.</td>
<td>Attorneys General must be notified not later than forty-five (45) days after determination of a security breach if more than 1,000 New Mexico residents are affected. Notification must include the number of New Mexico residents affected and a copy of the notification letter.</td>
<td></td>
<td>Attorney General may bring action to seek injunctive relief and award of damages for actual costs or losses, including consequential financial losses. If a court determines that a covered entity violated the statute knowingly or recklessly, the court may impose a civil penalty of up to $25,000 or $10.00 per instance of failed notification up to a maximum of $150,000.</td>
</tr>
</tbody>
</table>
Subject to statute: Any person or business which conducts business in New York state and which owns or licenses computerized data which includes private information.

Third party recipients: Any person or business that maintains computerized data which includes private information which such person or business does not own must notify the owner or licensee of any security breach involving private information immediately following discovery of the breach.

Written, electronic or telephonic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement).

- Notice to affected residents is required to contain specific content described in statute.
- Electronic notice permitted only when the consumer to be notified has consented to such notice. A log of all consumers notified electronically must be kept.
- Substitute notice is available by means prescribed in the statute if a business demonstrates to the state attorney general that the latter amount does not exceed $10,000 per instance of failed notification, provided that the latter amount may not exceed $150,000.

Other obligations: Any covered entity that must notify more than 5,000 New York residents at one time of a security breach is also required to notify consumer reporting agencies with notification procedures and timing that follow state law requirements.

Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted.

Safe harbor not available if the compromised data was encrypted with an encryption key that has also been acquired.

Substitute notice is available if the encryption was performed without the authorization of the data owner or the entity that maintained the data.

Attorney General and Department of State Police must be notified of a security breach without delaying notice to affected residents. The notification must describe timing, content and distribution of the notices to residents and the approximate number of affected persons.

Penalties:

Injunctive relief available, as well as actual costs or losses incurred by affected residents, including consequential financial losses.

For knowing or willful violations, civil penalties of the greater of $5,000 or up to $10,000 per instance of failed notification, provided that the latter amount may not exceed $150,000.

Private Cause of Action: No.

Sources:

Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.

Copyright © 2009-2018 Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.

Boston | London | Los Angeles | New York | San Diego | San Francisco | Washington | mintz.com
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>North Carolina</td>
<td>Information covered: Personal information of North Carolina. Definition includes (i) employer taxpayer identification numbers, (ii) Personal Identification (PIN) Code, (iii) biometric data, (iv) fingerprints, and (v) any other numbers or information that can be used to access a person’s financial resources. Personal information does 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. Important definitions: “Security Breach” means an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Access to encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. “Encryption” means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. Subject to statute: Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form, whether computerized, paper or otherwise. Third party recipients: Any business that maintains or possesses records or data containing personal information of North Carolina residents that the business does not own or license must notify the owner or licensee of the information of any security breach immediately following discovery of the breach consistent with law enforcement needs.</td>
<td>Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency requests delay in writing due to its determination that notification would impede a criminal investigation or jeopardize national or homeland security (in which case notification is delayed until authorized by law enforcement agency). Electronic notice allowed only when the consumer to be notified has consented to receipt of electronic communications. Notice to affected residents is required to contain specific content described in statute. Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, covered entity has insufficient contact information, or covered entity is unable to identify particular affected persons. Notice not required if the business responsible for the data concludes that the security breach is not reasonably likely to cause or create a “material risk of harm” to consumers. Other obligations: Any business that must notify more than 1,000 persons at one time of a security breach is also required to notify consumer reporting agencies without unreasonable delay.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Other exemptions: Exemption for good faith acquisition of personal information by employee or agent of a business for a legitimate purpose so long as personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure. Financial institutions subject to and in compliance with federal interagency guidelines, and credit unions subject to the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, are exempt.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Important definitions, cont’d: “Redaction” means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data.</td>
<td></td>
<td></td>
<td></td>
<td>Notification Procedures /</td>
<td></td>
<td>Penalties</td>
</tr>
<tr>
<td></td>
<td>Important definitions, cont’d: “Redaction” means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data.</td>
<td></td>
<td></td>
<td></td>
<td>Timing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Important definitions, cont’d: “Redaction” means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------------------------------------</td>
<td>--------------------------------</td>
<td>-----------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>North Dakota</td>
<td>Information covered: Personal information of North Dakota residents. Definition also includes (i) date of birth, (ii) mother’s maiden name, (iii) employee identification number in combination with any required access code or password, (iv) electronic or digitized signature, (v) health insurance information, and (vi) medical information.</td>
<td>Subject to statute: Any person that owns or licenses computerized data that includes personal information. Third party recipients: Any person that maintains or possesses records or data containing personal information that the person does not own or license must notify the owner or licensee of the information of any security breach immediately following discovery of the breach.</td>
<td>Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. Both the name information and associated data elements must be encrypted.</td>
<td>Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of the covered entity so long as personal information is not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the North Dakota statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the North Dakota statute. A financial institution, trust company or credit union subject to and in compliance with interagency guidance for unauthorized access to customer information and customer notice is deemed in compliance with North Dakota statute.</td>
<td>remedies for violations are set forth in N.D. Cent. Code 51-15.</td>
<td>Other exemptions, cont'd: A covered entity subject to HIPAA is deemed in compliance with North Dakota statute.</td>
</tr>
<tr>
<td>Return to Index of States</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Attorney General must be notified by mail or email if a single breach results in notice to more than 250 individuals.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------</td>
<td>----------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Ohio</td>
<td><strong>Information covered:</strong> Personal information of Ohio residents.</td>
<td><strong>Subject to statute:</strong> Any person, legal entity or business entity that conducts business in the state that owns or licenses computerized data that includes personal information.</td>
<td><strong>Written, electronic or telephonic notice must be provided</strong> to victims of a security breach within the most expedient time possible but <strong>no later than forty-five (45) days following the discovery of the breach</strong>, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement).</td>
<td><strong>Encryption Safe Harbor:</strong> Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted.</td>
<td><strong>Other exemptions:</strong> A covered entity subject to HIPAA is deemed in compliance with the Ohio statute.</td>
<td><strong>Penalties:</strong> Civil penalty of up to $1,000 for each day of non-compliance with statute, up to $5,000 per day after 60 days, and up to $10,000 per day after 90 days.</td>
<td><strong>Private Cause of Action:</strong> No.</td>
</tr>
<tr>
<td></td>
<td><strong>Important definitions:</strong> “Security Breach” means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information and that causes, or is reasonably believed to have caused or will cause, a material risk of identity theft or other fraud to a person or property of a resident of Ohio. “Encryption” means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. “Redacted” means altered or truncated so that no more than the last four digits of a social security number, driver’s license number, state identification card number, account number, or credit or debit card number is accessible as part of the data.</td>
<td><strong>Third party recipients:</strong> Any person that, on behalf of or at the direction of another person or governmental entity, is the custodian of or stores computerized data that includes personal information, must notify that other person or governmental entity of any security breach in an expeditious manner if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to an Ohio resident.</td>
<td>Such substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. Substitute notice also available to business entities with 10 employees or fewer that demonstrate costs will exceed $10,000.</td>
<td><strong>A determination of no likelihood of harm:</strong> Does not require notification to Attorney General.</td>
<td><strong>A waiver of the statute is void and unenforceable.</strong></td>
<td><strong>Encryption Safe Harbor:</strong> Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted.</td>
<td><strong>Other exemptions:</strong> A covered entity subject to HIPAA is deemed in compliance with the Ohio statute.</td>
</tr>
<tr>
<td></td>
<td><strong>Other obligations:</strong> Any covered entity that must notify more than 1,000 Ohio residents at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies without delaying notice to affected Ohio residents.</td>
<td><strong>Notification required solely in the case of breaches that have caused or are reasonably likely to cause a material risk of identity theft or other fraud to an Ohio resident.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Return to Index of States
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oklahoma</td>
<td>Click here to review text of statute (see Okla. Stat., Title 24, §§ 161 to 166). For specific rules applicable to state agencies – see Okla. Stat. §§ 74-3113.1.)</td>
<td>Information covered: Personal information of Oklahoma residents. Important definitions: “Security Breach” means unauthorized access and acquisition of unencrypted and redacted computerized data that compromises the security or confidentiality of personal information maintained as part of a database of personal information regarding multiple individuals and that causes, or the covered entity reasonably believes caused or will cause, identity theft or other fraud to any Oklahoma resident. “Encrypted” means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or rendering the data elements unreadable or unusable by other means. “Redact” means alteration or truncation of data such that no more than five digits of a social security number or the last four digits of a driver license number, state identification card number or account number are part of the data.</td>
<td>Subject to statute: An individual or entity that owns or licenses computerized information that includes personal information. Third party recipients: Any covered entity that maintains computerized data containing personal information that the covered entity does not own or license must notify the owner or licensee of the information of any security breach immediately as soon as practicable following discovery of the breach. Written, telephonic or electronic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement). Substitute notice is available by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information or does not have consent to provide notice otherwise. Notification required solely in the case of breaches that the covered entity reasonably believes has caused or will cause identity theft or other fraud to any Oklahoma resident.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. A breach must also be disclosed if the encryption key is compromised. Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Oklahoma statute if it maintains and complies with its own notification procedures as part of an information privacy or security policy and whose procedures are consistent with the timing requirements of the Oklahoma statute. A covered entity that complies with the notification requirements imposed by its primary or functional federal regulator is deemed in compliance with the Oklahoma statute.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General. Other exemptions, cont’d: Financial institutions subject to and in compliance with federal interagency guidelines are exempt.</td>
<td>Actual damages resulting from a violation of the statute or a civil penalty not to exceed $150,000 per breach. Violations of the statute by state-chartered or state-licensed financial institutions may only be enforced by the primary state regulator of the institution.</td>
<td>Privilege Cause of Action: No. Enforcement by Attorney General or a district attorney.</td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------</td>
<td>--------------------------------</td>
<td>---------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Oregon</td>
<td>Personal information of Oregon consumers.</td>
<td>Security Breach: Means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information.</td>
<td>Written, telephonic or electronic notice must be provided to victims of a security breach no later than 45 days from discovery of the breach unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement).</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise rendered unusable by other methods.</td>
<td>Oregon statute is exempt from exempt from Oregon’s statute.</td>
<td>Violations are an unlawful practice under ORS 646.607. Penalties can include $1,000 per violation. In the case of a continuing violation, each day’s continuance is a separate violation. Maximum penalty of $500,000.</td>
<td>Enforcement by the Director of the Department of Consumer and Business Services. If the director has reason to believe that any person has engaged in or is engaging in any violation of the Oregon statute, the director may issue a cease and desist order, or require the person to pay compensation to consumers injured by the violation. The director may order compensation to consumers only upon a finding that enforcement of the rights of the consumers by private civil action would be too burdensome or expensive as to be impractical.</td>
</tr>
<tr>
<td></td>
<td>Information covered:</td>
<td></td>
<td>Subject to statute: Any person, legal entity or public body (as defined in ORS 174.019) that owns, licenses, or otherwise possesses personal information that the person uses in the course of the person’s business, vocation, occupation or volunteer activities.</td>
<td>Other exemptions: Exemption for good faith and inadvertent acquisition of personal information by a covered entity or a covered entity’s employee or agent if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.</td>
<td>Attorney General must be notified electronically or by mail if a single breach affects 250 residents.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Important definitions:

- Security Breach: Means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information.
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pennsylvania</td>
<td>Information covered: Personal information of Pennsylvania residents. Important definitions: “Security Breach” means unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by a covered entity as part of a database of personal information regarding multiple individuals and that causes, or according to the covered entity’s reasonable belief has caused or will cause, loss or injury to any resident of Pennsylvania. “Encryption” means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. “Redacted” means altered or truncated so that no more than the last four digits of a social security number, driver’s license number, state identification card number, account number or financial account number is accessible as part of the data. Subject to statute: Any individual or business that maintains, stores or manages computerized data that contains personal information of Pennsylvania residents. Vendors: A vendor that maintains, stores or manages computerized data on behalf of a covered entity must provide notice of any breach of the security system following discovery of the breach.</td>
<td>Written, telephonic or e-mail notice (if a prior business relationship exists) must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • Substitute notice is available by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. • Notice not required if the covered entity responsible for the data concludes that the breach did not cause, or in its reasonable belief has not caused or is not likely to cause, loss or injury to any resident of Pennsylvania. • Notice only required if security breach materially compromises the security, confidentiality or integrity of personal information. Other obligations: Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Safe harbor is not available if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key. Other exemptions: Exemption for good faith acquisition by an employee or agent of a covered entity for the purposes of the covered entity so long as personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Pennsylvania statute if it maintains and complies with its own notification procedures as part of an information privacy or security policy and whose procedures are consistent with A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td>Violation of the statute constitutes an unfair or deceptive act in violation of the Unfair Trade Practices and Consumer Protection Law.</td>
<td>Private Cause of Action: No. Enforcement by Attorney General only.</td>
<td></td>
</tr>
</tbody>
</table>
### Rhode Island

#### Information covered:
Personal information of Rhode Island residents when the name and the data elements are not encrypted or are in hard copy, paper format.

**Important definitions:**
- **“Security Breach”** means unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information.
- **“Encrypted”** means the transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Data will not be considered to be encrypted if it is acquired in combination with any key, security code or password that would permit access to encrypted data.

#### Subject to statute:
Any person or legal commercial entity that stores, owns, collects, processes, maintains, acquires, uses or licenses data that includes personal information.

#### Third party recipients:
Refer to covered entities subject to statute to determine if a third party recipient of personal information is implicated.

A covered entity that discloses computerized unencrypted personal information about a Rhode Island resident pursuant to a contract with a nonaffiliated third party must require by contract that the third-party implement and maintain reasonable security procedures and practices to protect the personal information.

### Written or electronic notice must be provided to victims of a security breach within the most expedient time possible but no later than forty-five (45) calendar days after confirmation of the breach and ability to ascertain information for notice unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).

- **Notice to affected residents is required to contain specific content described in statute.**
- **Substitute notice is available by means prescribed in the statute if costs to exceed $25,000, affected class exceeds 50,000 persons, or covered entity has insufficient contact information.**
- **Notification not required if security breach does not pose a significant risk of identity theft.**

#### Other obligations:
- **A person or business that owns or licenses computerized unencrypted personal information about a Rhode Island resident must implement and maintain a risk-based information security program that contains reasonable security procedures and practices to protect personal information.**
- **Any covered entity that must notify more than 500 residents at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.**

### Attorney General must be notified if a single breach affects more than 500 residents.

**Notification will include information about timing, content, distribution of notices and approximate number of affected individuals.**

### Other exemptions:
- **A covered entity is deemed in compliance with the Rhode Island statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Rhode Island statute.**
- **A covered entity subject to HIPAA is deemed in compliance with Rhode Island’s statute.**
- **A financial institution, trust company or credit union in violation for which a penalty of not more than $100 per record may be imposed. Each knowingly and willful violation of a civil violation for which a penalty of not more than $200 may be imposed.**

### Penalties:
Each reckless violation is a civil violation for which a penalty of not more than $100 per record may be imposed. Each knowingly and willful violation of a civil violation for which a penalty of not more than $200 may be imposed.

### Enforcement by Attorney General only.
### State / Link to Statute

Return to Index of States

| South Carolina Click here to review text of statute (see S.C. Code §39-1-90). |

<table>
<thead>
<tr>
<th>Information Covered / Important Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>“Health Insurance Information”</strong> means an individual’s health insurance policy number, subscriber identification number or any unique identifier used by a health insurer to identify the individual.</td>
</tr>
<tr>
<td><strong>Information covered:</strong> Personal information of South Carolina residents. Definition also includes other numbers or information which may be used to access a person’s financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely identify an individual.</td>
</tr>
<tr>
<td><strong>Important definitions:</strong> “Security Breach” means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction or other methods that compromise the security, confidentiality or integrity of the personal information, 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.</td>
</tr>
<tr>
<td><strong>Third party recipients:</strong> A person conducting business in South Carolina and maintaining computerized data or other data that includes personal identifying information.</td>
</tr>
<tr>
<td><strong>Subject to statute:</strong> A person or legal entity (including cooperative or association) conducting business in South Carolina and owning or licensing computerized data or other data that includes personal identifying information.</td>
</tr>
</tbody>
</table>

### Covered Entities / Third Party Recipients

<table>
<thead>
<tr>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Written, electronic or telephonic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement).</td>
</tr>
<tr>
<td>• Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.</td>
</tr>
<tr>
<td>• Notification only required when illegal use of the personal data acquired has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.</td>
</tr>
</tbody>
</table>

### Other obligations:

- Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.

### Encryption Safe Harbor / Other Exemptions

- **Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise rendered unusable or unusable.

### Notice to Regulator / Waiver

- **Other exemptions:** Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of its business so long as personal information is not used or subject to further unauthorized disclosure.

### Penalties

- **A covered entity is deemed in compliance with the South Carolina statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the South Carolina statute.**

### Private Cause of Action / Enforcement

- **A resident of South Carolina who is injured by a violation may institute a civil action to seek an injunction and to recover damages and attorneys’ fees and costs, if successful.**
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Dakota Click here to review text of statute.</td>
<td><strong>Information covered:</strong> Personal information of South Dakota residents. Definition includes usernames and passwords, financial information, personal identification numbers (“PINs”) or other access codes for financial accounts, medical information, health insurance information, and identification number assigned by an employer in combination with any required security code, access code, password, or biometric data. Also covers “protected information,” which includes user name or email address with access code for online accounts, and account number or credit or debit card number, in combination with any access code for financial accounts. <strong>Important definitions:</strong> “Breach of Security” means the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder.</td>
<td><strong>Subject to statute:</strong> A person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information of Alabama residents. <strong>Third party recipients:</strong> Third parties maintaining personal information on behalf of a covered entity must notify covered entity about a breach and cooperate as necessary to allow covered entity to comply with statute. The covered entity must satisfy all further notification obligations under the statute. <strong>Written or electronic notice must be provided to victims of a security breach as expeditiously as possible and without unreasonable delay, but no later than sixty (60) days following the discovery of the breach unless law enforcement agency determines that disclosure will interfere with a criminal investigation (in which case notification delayed until authorized by law enforcement). Notice to affected residents is required to contain specific content described in statute:</strong> • If a delay in notification is prompted by law enforcement needs, notice to affected residents must occur 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. • Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • Notice not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a reasonable likelihood of harm to the consumers whose personal information was acquired. The determination must be documented in writing and maintained for three years. <strong>Other Obligations:</strong></td>
<td><strong>Encryption Safe Harbor:</strong> Statute not applicable if the personal information that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. <strong>Other exemptions:</strong> Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as the personal information is not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the South Dakota statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Tennessee statute. A covered entity that is subject to GLBA or HIPAA is exempt from South Dakota’s statute.</td>
<td>Financial institutions subject to and in compliance with federal interagency guidelines are deemed in compliance with the South Carolina statute.</td>
<td>In addition to any remedy provided under SD § 37-24-6, violations by non-governmental entities are liable for civil penalties up to $10,000 per day per violation.</td>
<td><strong>Private Cause of Action:</strong> No. Enforcement by Attorney General only.</td>
<td></td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------</td>
<td>----------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td><strong>Tennessee</strong></td>
<td>Information covered: Personal information of Tennessee residents. <strong>Important definitions:</strong> &quot;Encrypted&quot; means computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2. &quot;Security Breach&quot; means unauthorized 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. &quot;Unauthorized Person&quot; includes an employee of a covered entity who is discovered to have obtained personal information and intentionally used it for an unlawful purpose. <strong>Subject to statute:</strong> Any person or business that conducts business in Tennessee. <strong>Third party recipients:</strong> Any covered entity that maintains computerized data that includes personal information that the covered entity does not own must notify the owner or licensee of the information of any security breach immediately following discovery of the breach but no later than forty-five (45) days from when the breach became known to third party recipient. <strong>Written or electronic notice must be provided to victims of a security breach immediately but no later than forty-five (45) days following the discovery or notification to covered entity of a security breach, unless a law enforcement agency determines that notice will impede a criminal investigation in which case notification is delayed until authorized by law enforcement but still must occur within forty-five (45) days after the law enforcement agency’s authorization.</strong> • If a delay in notification is prompted by law enforcement needs, notification to affected residents must occur no later than forty-five (45) days after law enforcement agency determines that notification will no longer compromise its investigation. • Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. • Notice only required if security breach materially compromises the security, confidentiality or integrity of personal information. <strong>Other obligations:</strong> Any covered entity that must notify more than 1,000 persons at one time of a security breach is <strong>Encryption Safe Harbor:</strong> Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized person is fully encrypted. Safe harbor not available if the encryption key is compromised together with the encrypted data. <strong>Other exemptions:</strong> Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as the personal information is not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Tennessee statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Tennessee statute. <strong>A determination of no likelihood of harm:</strong> Does not require notification to Attorney General. <strong>Violations fall under the Tennessee Consumer Protection Act and constitute an unfair or deceptive act or practice affecting trade or commerce.</strong> <strong>Residents and business entities injured by a violation may institute a civil action to recover damages as well as injunctive relief.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Return to Index of States

Click here to review text of statute (see Tenn. Code, Titel 47, §47-18-2107, et seq.)
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Texas</td>
<td>Information covered: Personal information of Texas residents. (Texas uses the defined term “sensitive personal information.”) Definition also includes: (i) information about physical or mental health or condition, (ii) the provision of health care to the individual, or (iii) the payment for the provision of health care to the individual.</td>
<td>Third party recipients: A person who maintains computerized data that includes sensitive personal information.</td>
<td>Written or electronic notice must be provided to victims of a security breach as quickly as possible, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). • Texas statute allows entities from states other than Texas to provide notice to individuals under the other states’ law or under Texas law, provided the other state has regulations that require notification of a breach to affected persons. • Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. Safe harbor not available if personal data is encrypted but the encryption key is compromised by security breach.</td>
<td>Other exemptions: Exemption for good faith acquisition of sensitive personal information by an employee or agent of the covered entity for the purposes of the covered entity so long as the sensitive personal information is not used or disclosed in an unauthorized manner. A person is deemed in compliance with the Texas statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing.</td>
<td>Civil penalty of at least $2,000 but not more than $50,000 for each violation. Failure to take reasonable corrective action to comply with the statute can result in additional penalties of $100 per individual per day of failed or delayed notification, not to exceed $250,000 for a single breach. The Attorney General may also seek injunctive and other equitable relief, as well as reasonable expenses, including attorney’s fees, court costs, and investigatory costs.</td>
<td>Private Cause of Action: No. Enforcement by Attorney General only.</td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------</td>
<td>----------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Utah</td>
<td>Information covered: Personal information of Utah residents.</td>
<td>Subject to statute: Any person who owns or licenses computerized data that includes personal information concerning a Utah resident. <strong>Important definitions:</strong> “Security breach” means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality or integrity of personal information. <strong>Third party recipients:</strong> A person who maintains computerized data that includes personal information that the person does not own must notify and cooperate with the owner or licensor of the information of any security breach immediately following discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur. <strong>Written, telephonic or electronic notice must be provided</strong> to victims of a security breach following a prompt investigation within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). - Notice may also be completed by publishing notice of the security breach in a newspaper of general circulation and as required in Utah Code §451-101. - <strong>Notification is only required</strong> if the covered entity determines that misuse of the personal information is so long as personal information is not used for an unlawful purpose or disclosed in an unauthorized manner. - <strong>Other obligations:</strong> Any person who conducts business in Utah and maintains personal information must implement and maintain reasonable procedures to protect personal information and ensure proper destruction of records containing personal information that no longer need to be retained with methods such as shredding, erasing or otherwise modifying personal information such that it is indecipherable.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or protected by another method that renders the data unreadable or unusable. <strong>A determination of no likelihood of harm:</strong> Does not require notification to Attorney General. <strong>A waiver</strong> of the statute is void and unenforceable.</td>
<td>Civil fines no greater than $2,500 per violation or series of violations concerning a specific consumer, and no greater than $100,000 in the aggregate for related violations concerning more than one consumer. Injunctive relief is also available.</td>
<td>Private Cause of Action: No. Enforcement by Attorney General only.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Information covered: Personal identifying information of Vermont residents. Vermont’s variation on the defined term includes the typical data elements in this chart’s definition of personal information.

Important definitions:
- “Security Breach” means 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.
- “Encryption” means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.
- “Redaction” means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

Subject to statute: Person, legal or commercial entity, private universities or any other entity that maintains or possesses computerized data containing personally identifiable information of a consumer.

Third party recipients: Any covered entity that maintains or possesses personally identifiable information of a consumer that the covered entity does not own or license, or any covered entity that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information that the covered entity does not own or license. Must notify the owner or licensee of the information of any security breach immediately following discovery of the breach consistent with law enforcement needs.

Written, telephonic or electronic notice must be provided to victims of a security breach following a prompt investigation within the most expedient time possible and without unreasonable delay, but not later than forty-five (45) days after discovery of the breach or notification from a third party, unless a delay is requested by a law enforcement agency concerned that disclosure will impede a law enforcement investigation or jeopardize public safety or national or homeland security interests (in which case notification is delayed until authorized by the law enforcement agency).

- Electronic notice only permitted under certain conditions.
- Notice to affected residents is required to contain specific content described in statute.
- Substitute notice is available by means prescribed in the statute if costs to exceed $5,000, affected class exceeds 5,000 persons, or covered entity has insufficient contact information.
- Notice not required if covered entity establishes that misuse of personal information is not reasonably possible and covered entity provides notice of such determination to the Attorney General.

Other obligations: Any covered entity that must notify more than 1,000 persons at one time of a security breach is

Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or protected by another method that renders the data unreadable or unusable.

Other exemptions: Exemption for good faith acquisition of personally identifying information by an employee or agent of a covered entity for a legitimate purpose so long as the personally identifiable information is not used for a purpose unrelated to the covered entity’s business or subject to further unauthorized disclosure.

Financial institutions subject to certain federal interagency guidance regarding consumer information are exempt.

Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or protected by another method that renders the data unreadable or unusable.

Other exemptions: Exemption for good faith acquisition of personally identifying information by an employee or agent of a covered entity for a legitimate purpose so long as the personally identifiable information is not used for a purpose unrelated to the covered entity’s business or subject to further unauthorized disclosure.

Financial institutions subject to certain federal interagency guidance regarding consumer information are exempt.

The statute requires that no more than 1,000 persons at one time of a security breach is subject if it complies with notification requirements or procedures imposed by its primary or functional federal regulator.
**State / Link to Statute** | **Information Covered / Important Definitions** | **Covered Entities** / Third Party Recipients | **Notice Procedures & Timing / Other Obligations** | **Encryption Safe Harbor / Other Exemptions** | **Notification to Regulator / Waiver** | **Penalties** | **Private Cause of Action / Enforcement**
---|---|---|---|---|---|---|---
Return to Index of States | Virginia | Click here to review text of statute. | **Information covered:**
Personal information of Virginia residents.

**Important definitions:**

- “Security Breach” means 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 a Virginia resident.

- “Encrypted”: Means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.

- “Redact” means alteration or truncation of data such that no more than five digits of a social security number or the last four digits of a driver’s license number, state identification card number, or account number is required to notify without unreasonable delay consumer reporting agencies.

- **Third party recipients:** Any covered entity that maintains computerized data that includes personal information that the covered entity does not own or license must notify the owner or licensee of the information of any security breach without unreasonable delay following discovery of the breach.

- **Subject to statute:** Any individual, legal or commercial entity that owns or licenses computerized data that includes personal information.

- **Written, telephonic or electronic notice must be provided:** To victims of a security breach without unreasonable delay, unless disclosure impedes law enforcement investigation (in which case notification is delayed until authorized by the law enforcement agency).

- **Notice to affected residents is required to contain specific content described in statute.**

- **Substitute notice is available:** By means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information or does not have consent to provide notice by primary means.

- **Notice only required if the security breach causes, or the covered entity reasonably believes has caused, or will cause, identity theft or other fraud to a Virginia resident.**

- **Other obligations:** Any person that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies and the Attorney General.

- **Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Safe harbor not available if personal information is encrypted but the encryption key is compromised.

- **Other exemptions:** A covered entity is deemed in compliance with the Virginia statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the Virginia statute.

- **Attorney General must be notified of a security breach:** A determination of no likelihood of harm:

- **A determination of no likelihood of harm:** Does not require notification to Attorney General.

- **Employers or payroll service providers who experience a security breach containing a taxpayer identification number in combination with the income tax withheld must notify the Department of Taxation if breach involves payroll information.**

- **Individuals may bring an action to recover direct economic damages resulting from a violation of the Virginia statute.**

- **Attorney General may bring an action and may impose a civil penalty not to exceed $150,000 per security breach or a series of breaches of a similar nature that are discovered in a single investigation.**

- **Violations by state-chartered or licensed financial institutions are redressed by its primary state regulator.**

- **Violations by insurance companies are redressed by the State Corporation commission.**

<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Washington</td>
<td>Information covered: Personal information of Washington residents.</td>
<td>Important definitions: “Security Breach” means unauthorized acquisition of data (in any form) that compromises the security, confidentiality or integrity of personal information maintained by the person or business. “Secured” means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable or undecipherable.</td>
<td>Subject to statute: Any person or business that conducts business in Washington and that owns or licenses data (in any form) that includes personal information.</td>
<td>Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, but not later than forty-five (45) days after discovery of the security breach, unless a law enforcement agency determines that notice will impede an investigation (in which case notification is delayed until authorized by law enforcement). Notice to affected residents is required to contain specific content described in statute. Substitute notice is available by means prescribed in the statute if costs to exceed $250,000, affected class exceeds 500,000 persons, or covered entity has insufficient contact information. Notice not required if the security breach is not reasonably likely to subject consumers to a risk of harm.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is secured (e.g. encryption or redaction). Safe harbor not available if a confidential process, encryption key or other means to decipher the secured information is compromised. Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity for the purposes of the covered entity so long as the personal information is not used or subject to further unauthorized disclosure. A covered entity is deemed in compliance with the Washington statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures</td>
<td>Attorney General must be notified at the same as notice to residents if a single breach results in notification to more than 500 residents. Notification must be submitted electronically and include the number (or estimate) of affected Washington residents and a sample copy of the notification to consumers. A determination of no likelihood of harm: Does not require notification to Attorney General. A waiver of the statute is void and unenforceable.</td>
<td>Violations are an unfair or deceptive act in trade or commerce and an unfair method of competition.</td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------</td>
<td>-----------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>West Virginia</td>
<td>Information covered: Personal information of West Virginia residents. Important definitions: &quot;Security Breach&quot; means unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the security breach has caused or will cause identity theft or other fraud to any resident of West Virginia. &quot;Encrypted&quot; means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key or securing the information by another method that renders the data elements unreadable or unusable. &quot;Redact&quot; means alteration or truncation of data such that no more than the last four digits of a social security number, driver’s license number, state driver’s license number, state</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| | Subject to statute: An individual or legal or commercial entity that owns or licenses computerized data that includes personal information. Third party recipients: Any covered entity that maintains computerized data that includes personal information that the covered entity does not own or license must notify the owner or licensee of the information of any security breach as soon as practicable following discovery of the breach. | written, telephonic or electronic notice must be provided to victims of a security breach without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement).  
- Notice to affected residents is required to contain specific content described in statute.  
- Substitute notice is available by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information.  
- Notification is only required if the covered entity reasonably believes the security breach has caused or will cause identity theft or other fraud to any West Virginia resident. Other obligations: Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies. | Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted or redacted. Safe harbor not available if personal information is encrypted but the encryption key is compromised. Other exemptions: A covered entity is deemed in compliance with the West Virginia statute if it maintains computerized data that includes personal information and whose procedures are consistent with the timing requirements of the West Virginia statute. A covered entity is deemed in compliance with the West Virginia statute if it complies with notification requirements or procedures imposed by its primary or functional federal regulator that are at least as | | | |

Other exemptions:
- A covered entity is deemed in compliance with the West Virginia statute if it maintains computerized data that includes personal information and whose procedures are consistent with the timing requirements of the West Virginia statute.
- A covered entity is deemed in compliance with the West Virginia statute if it complies with notification requirements or procedures imposed by its primary or functional federal regulator that are at least as

A determination of no likelihood of harm: Does not require notification to Attorney General.

A covered entity is deemed in compliance with the West Virginia statute if it maintains computerized data that includes personal information and whose procedures are consistent with the timing requirements of the West Virginia statute.

A covered entity is deemed in compliance with the West Virginia statute if it complies with notification requirements or procedures imposed by its primary or functional federal regulator that are at least as

Cryptographic Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is "encrypted" or redacted. Safe harbor not available if personal information is encrypted but the encryption key is compromised.

Other exemptions:
- A covered entity is deemed in compliance with the West Virginia statute if it maintains computerized data that includes personal information and whose procedures are consistent with the timing requirements of the West Virginia statute.
- A covered entity is deemed in compliance with the West Virginia statute if it complies with notification requirements or procedures imposed by its primary or functional federal regulator that are at least as

A determination of no likelihood of harm: Does not require notification to Attorney General.

Penalties:
- No civil penalty will exceed $150,000 per breach or series of breaches of a similar nature that are discovered in a single investigation.
- Violations by financial institutions will be redressed by their primary regulator.

Private Cause of Action: No enforcement by Attorney General only.
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wisconsin</td>
<td>Information covered: Personal information of Wisconsin residents. Definition includes (i) an individual’s DNA data, and (ii) unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.</td>
<td>Subject to statute: An entity whose principal place of business is located inside Wisconsin, or an entity located outside Wisconsin that maintains or licenses personal information in Wisconsin. Includes entities that maintain a depository account for a resident or lends money to a resident.</td>
<td>Notice to victims of a security breach within a reasonable time not to exceed forty-five (45) days after discovery of the security breach, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland security (in which case notification is delayed until authorized by law enforcement). • Notice may be provided by mail or by a method the entity has previously employed to communicate with the affected persons. Upon written request from an affected person, the covered entity must identify the personal information that was acquired. • Substitute notice is available by means described in statute if a covered entity cannot with reasonable diligence determine the mailing address of the subject of the personal information compromised. • Notice not required if the security breach does not create a material risk of identity theft or fraud to the affected persons. Other obligations: Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted, redacted or otherwise altered in a manner that renders it unreadable. Other exemptions: Exemption for good faith acquisition of personal information by an employee or agent of a covered entity if it is used solely for a lawful purpose. Financial institutions regulated by certain federal laws described in the statute are exempt. Entities covered by HIPAA are exempt.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td>Private Cause of Action: No.</td>
<td></td>
</tr>
</tbody>
</table>
### Wyoming

**Click here to review text of statute (see Stat., Title 40, Chapter 12 §§40-12-501, et seq.)**

<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wyoming</strong></td>
<td>Personal identifying information about a resident of Wyoming.</td>
<td>Subject to statute: Any individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming.</td>
<td>Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement).</td>
<td>Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is redacted.</td>
<td>A determination of no likelihood of harm: Does not require notification to Attorney General.</td>
<td>Actions in law or equity permitted to ensure compliance with Wyoming statute and to recover damages.</td>
<td>Private Cause of Action: No.</td>
</tr>
<tr>
<td><strong>Click here to review text of statute (see Stat., Title 40, Chapter 12 §§40-12-501, et seq.)</strong></td>
<td><strong>Important definitions:</strong> “Security Breach” means an unauthorized acquisition of computerized data that includes personal identifying information about a resident of Wyoming.</td>
<td><strong>Third party recipients:</strong> Any covered entity that maintains computerized data that includes personal identifying information that the covered entity does not own or license must notify the owner or licensee of the information of any security breach as soon as practicable following discovery of the breach.</td>
<td><strong>Important definitions, cont’d:</strong> Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal or civil investigation or jeopardize homeland or national security (in which case notification is delayed until authorized by law enforcement).</td>
<td><strong>Encryption Safe Harbor:</strong> Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is redacted.</td>
<td><strong>A determination of no likelihood of harm:</strong> Does not require notification to Attorney General.</td>
<td><strong>Actions in law or equity permitted to ensure compliance with Wyoming statute and to recover damages.</strong></td>
<td><strong>Private Cause of Action: No.</strong></td>
</tr>
</tbody>
</table>

**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is redacted.

**A determination of no likelihood of harm:** Does not require notification to Attorney General.

**Actions in law or equity permitted to ensure compliance with Wyoming statute and to recover damages.**

**Private Cause of Action: No.**

**Encryption Safe Harbor:** Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is redacted.

**A determination of no likelihood of harm:** Does not require notification to Attorney General.

**Actions in law or equity permitted to ensure compliance with Wyoming statute and to recover damages.**

**Private Cause of Action: No.**
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>District of Columbia</td>
<td>Information covered: Personal information of District of Columbia residents. Definition includes any 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. Important definitions: “Security Breach” means unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data, that compromises the security, confidentiality or integrity of personal information maintained by the person or business. Subject to statute: Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information. Third party recipients: Any covered entity who maintains, handles or otherwise possesses computerized or other electronic data that includes personal information.</td>
<td>Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). Substitute notice is available by means prescribed in the statute if costs to exceed $50,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. Other obligations: Any covered entity that must notify more than 1,000 persons at one time of a security breach is also required to notify without unreasonable delay consumer reporting agencies.</td>
<td>Encryption Safe Harbor: None. Other exemptions: A covered entity is deemed in compliance with the District of Columbia statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the District of Columbia statute. Any covered entity subject to GLBA is exempt.</td>
<td>A waiver of the statute is void and unenforceable.</td>
<td>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 is a separate violation. Attorney General may also bring petition for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by District of Columbia residents. Any District of Columbia resident may bring a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages may not include dignitary damages, including pain and suffering.</td>
<td>Private Cause of Action: Yes. Enforcement by Attorney General and individuals.</td>
<td></td>
</tr>
<tr>
<td>State / Link to Statute</td>
<td>Information Covered / Important Definitions</td>
<td>Covered Entities / Third Party Recipients</td>
<td>Notice Procedures &amp; Timing / Other Obligations</td>
<td>Encryption Safe Harbor / Other Exemptions</td>
<td>Notification to Regulator / Waiver</td>
<td>Penalties</td>
<td>Private Cause of Action / Enforcement</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------</td>
<td>----------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Puerto Rico</td>
<td>Information covered: Personal information of Puerto Rico residents. Definition includes (i) names of users and passwords or access codes to public or private information systems, (ii) medical information protected by HIPAA, (iii) tax information, and (iv) work-related evaluations. Mailing and residential addresses are not included in the definition.</td>
<td>Subject to statute: Any entity that is the proprietor or custodian of a database that includes personal information of citizen residents of Puerto Rico. Third party recipients: Any entity that as part of its operations resells or provides access to digital data banks that at the same time contain personal information files of Puerto Rico citizens must notify the proprietor, custodian or holder of the information of any security breach. Written direct notice or authenticated electronic notice must be provided to victims of a security breach as expeditiously as possible, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement). Notice to affected persons is required to contain specific content described in statute. Substitute notice is available by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 100,000 persons, or covered entity has insufficient contact information. Substitute notice may be available in other situations if notification is unduly onerous or difficult.</td>
<td>Encryption Safe Harbor: Statute only applies to data that is not protected by a special cryptographic code. Department of Consumer Affairs must be notified of any security breach within ten (10) days of detection of security breach. The Department will make a public announcement about security breach within 24 hours of receiving notification from the covered entity.</td>
<td>Fines of $500 up to a maximum of $5000 for each violation.</td>
<td>Fines of $500 up to a maximum of $5000 for each violation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Important definitions: “Security Breach” means any situation in which it is detected that access to personal information has been permitted to unauthorized persons or entities so that the security, confidentiality or integrity of the information has been compromised; or, when those persons authorized to access personal information may have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. The definition includes both physical and electronic intrusions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Private Cause of Action: Yes. Consumers may bring actions in a competent court for damages.</td>
</tr>
</tbody>
</table>

[Click here to review text of statute (see Laws of Puerto Rico, Title 10, Subtitle 3, Chapter 310, §4051 et seq.).]
<table>
<thead>
<tr>
<th>State / Link to Statute</th>
<th>Information Covered / Important Definitions</th>
<th>Covered Entities 1 / Third Party Recipients</th>
<th>Notice Procedures &amp; Timing / Other Obligations</th>
<th>Encryption Safe Harbor / Other Exemptions</th>
<th>Notification to Regulator / Waiver</th>
<th>Penalties</th>
<th>Private Cause of Action / Enforcement</th>
</tr>
</thead>
</table>
| Virgin Islands          | Information covered: Personal information of Virgin Islands residents. | Subject to statute: Any person or business that conducts business in the Virgin Islands, and that owns or licenses computerized data that includes personal information. | Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless a law enforcement agency determines that notice will impede a criminal investigation (in which case notification is delayed until authorized by law enforcement).  
- Substitute notice is available by means prescribed in the statute if costs to exceed $100,000, affected class exceeds 50,000 persons, or covered entity has insufficient contact information. | Encryption Safe Harbor: Statute not applicable if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. | A waiver of the statute is void and unenforceable. | Businesses that violate the statute may be enjoined.  
Customers injured by a violation may commence a civil action to recover damages. | Private Cause of Action: Yes. |

1 Click here to review text of statute (see V.I. Code, Title 14, Chapter 110, Subchapter I, §2209 et seq.)

2 Return to Index of States