

Status of Data Breach Statutes in the 50 States
Originally prepared by K.M. Das, Davis Wright Tremaine LLP;
revised by Marti Arvin, Privacy Officer, University of Louisville.
Used with permission.

| State | Statute Enacted | | Summary | Notes |
|---------|-----------------|----|---|--|
| | Yes | No | | |
| Alabama | | X | <p>Existing law does not require a person that owns, licenses, or maintains data containing the personal information of an Alabama resident to notify the resident if the personal information is disclosed to an unauthorized person.</p> <p>This bill would require a person that owns or licenses computerized data containing the personal information of an Alabama resident to notify the resident of a breach of security involving the personal information.</p> <p>This bill would provide for notification of breaches of security by third-party persons that maintain computerized data containing personal information on behalf of the person who owns or licenses the computerized data.</p> <p>This bill would provide limited exceptions for the time and manner of the notification. (Text from S.B. 114.)</p> | Alabama's S.B. 114 has been referred to the Judiciary Committee. |
| Alaska | | X | <p>An Act relating to breaches of security involving personal information, consumer report security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, disposal of records, factual declarations of innocence after identity theft, filing police reports regarding identity theft, furnishing consumer credit header information, and truncation of credit and debit card information; and amending Rule 60, Alaska Rules of Civil Procedure.</p> <p>Proposed Legislation</p> <p>H.B. 31 Relates to breaches of security involving personal information, credit report and credit score security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, care of records, disposal of records, identity theft, furnishing consumer credit header information, credit cards, and debit cards, and to the jurisdiction of the office of administrative hearings; amends Rule 60, Alaska Rules of Civil Procedure.</p> <p>S.B. 21 Relates to breaches of security involving personal information, credit report and credit score security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, care of records, disposal of records, identity theft, furnishing consumer credit header information, credit cards, and debit cards, and to the jurisdiction of the office of administrative hearings; amends Rule 60, Alaska Rules of Civil Procedure.</p> | Alaska's S.B. 222 has been referred to the Finance Committee. |

| State | Statute Enacted | | Summary | Notes |
|----------|-----------------|----|---|--|
| | Yes | No | | |
| Arizona | X | | <p>Requires a person conducting business in Arizona that owns or licenses unencrypted computerized data that includes personal information that becomes aware of an incident of unauthorized acquisition of and access to unencrypted or unredacted computerized data to conduct an investigation to promptly determine if a breach of the security system has occurred.</p> <p>If the investigation results in a determination that there has been a breach, the person shall notify the individuals affected in the most expedient manner possible, without unreasonable delay. The notice provided can be written notice, electronic notice, or telephonic notice. If the cost of providing notice would exceed \$50,000 or more than 100,000 persons would have to be informed, substitute notice—including electronic notice if the person has the affected individual’s email address and notification to statewide media—may be given.</p> <p>The definition of person includes governmental agencies, but excludes law enforcement agencies, prosecution agencies, and courts.</p> <p>Proposed legislation SB 1042 Excludes the Department of Public Safety, a county sheriff's department and municipal police departments from requirements regarding notification of a breach of a security system and the possible compromise of personal information</p> | S.B. 1338 was approved by the governor on April 26, 2006. |
| Arkansas | X | | <p>A person or business must take all reasonable steps to destroy customer records, which are no longer to be retained. A person or business that acquires, owns or licenses personal information about a resident must also implement and maintain reasonable security procedures to prevent unauthorized access.</p> <p>Any person or business that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, a person or business that maintains such data must notify the owner or licensee of the information. Notice is not required if after a reasonable investigation, there is no likelihood of harm to customers.</p> <p>The proper procedure and timing for giving notice is provided by statute. However, a person or business that maintains its own notification procedures, that are consistent with the statute’s timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach.</p> <p>An exemption exists for any person or business that is regulated by a state or federal laws providing greater protection to personal information and at least as thorough disclosure requirements. A waiver of the statute’s provisions is unenforceable.</p> <p>A violation is punishable by the Attorney General as a deceptive trade practice under ARK. CODE ANN. §§ 4-88-101 through 4-88-115.</p> | <p>S.B. 1167 was approved by the Governor on March, 31, 2005. The effective date of the Bill was not provided in the Bill text of history.</p> <p>The Bill is to be codified at ARK. CODE ANN. §§ 4-110-101 through 4-110-108.</p> |

| State | Statute Enacted | | Summary | Notes |
|------------|-----------------|----|---|---|
| | Yes | No | | |
| California | X | | <p>The following entities must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person: (1) any agency that owns or licenses computerized data that includes personal information, and (2) any person or business conducting business in California that owns or licenses computerized data that includes personal information. In the event of a breach, any agency, person, or business that maintains such data must notify the owner or licensee of the information.</p> <p>The proper procedure and timing for giving notice is provided by statute. However, a person or business that maintains its own notification procedures, that are consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach.</p> <p>A waiver of the statute's provisions is unenforceable.</p> <p>In addition to any other rights and remedies available under the law, any customer injured by a violation may institute a civil action to recover damages. Moreover, any business that violates or proposes to violate the statute may be enjoined from doing so.</p> | <p>A.B. 700 was signed by the Governor on September 29, 2002, and became effective as of July 1, 2003.</p> <p>The Bill is codified at CAL. CIV. CODE §§ 1798.29, and 1798.82 through 1798.84.</p> |
| Colorado | X | | <p>An individual or commercial entity that conducts business in Colorado <i>and</i> that owns or licenses computerized data that includes personal information about a reside of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or the commercial entity shall give notice as soon as possible to the affected Colorado resident unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.</p> <p>Notice means: written notice, telephonic notice, or electronic notice. Substitute notice—email notice, conspicuous posting on website, and notification to major statewide media—can be employed if the cost of providing notice would exceed \$250,000 or 200,000 Colorado residents would have to be individually notified.</p> <p>If more than 100,000 Colorado residents have to be notified, the individual or commercial entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the anticipated date of the notification and the approximate number of residents who are to be notified. The individual or commercial entity shall not be required to provide to the consumer reporting agencies the names of the affected Colorado residents.</p> | <p>HB 06-1119 was signed into law by the Governor on April 24, 2006.</p> |

| State | Statute Enacted | | Summary | Notes |
|-------------|-----------------|----|---|---|
| | Yes | No | | |
| Connecticut | X | | <p>Subject to certain conditions and exemptions, a consumer may submit a written request to place a security freeze on their credit report.</p> <p>Any person or business (conducting business in the state) who in the ordinary course of business, owns, licenses, or maintains computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notice is not required if after investigation and consultation with relevant agencies, there is no reasonable likelihood of harm to customers. In the event of a breach, a person that only maintains such data must notify the owner or licensee of the information.</p> <p>The proper procedure and timing for giving notice is provided by statute. However, compliance with the notice requirement is satisfied if subject persons are notified: (1) according to a person or business' own notification procedures, consistent with the statute's timing requirements; or (2) according to a security breach procedure pursuant to the guidelines of the primary or functional regulator.</p> <p>Failure to comply constitutes an unfair trade practice under CONN. GEN. STAT. § 42-110b, and shall be enforced by the Attorney General.</p> | <p>S.B. 650 was approved by the Governor on June 24, 2005, and becomes effective on January 1, 2006.</p> <p>The statutory codification of the Bill does not appear to have been determined.</p> |
| Delaware | X | | <p>Any individual or commercial entity (conducting business in Delaware) that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, an individual or commercial entity that maintains such data must notify the owner or licensee of the information. If notice is required, written notification of the nature and circumstances of the breach must also be provided to the Consumer Protection Division of the Department of Justice. The proper procedure and timing for giving notice is provided by statute. However, a person or business that maintains its own notification procedures, that are consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach. If an individual or commercial entity is regulated by State or federal laws providing greater protection, compliance with that law also suffices.</p> <p>In addition to other rights provided by law, a Delaware resident damaged by a violation is granted a private right of action to recover damages. If damages are awarded, the damages shall be triple the amount of actual damages plus reasonable attorney fees. The Attorney General may also bring an action in law or equity for other appropriate relief. The provisions of the statute are not exclusive and do not relieve an individual or commercial entity from compliance with other applicable provisions of law. A violation is within the scope of the enforcement duties and powers of the Consumer Protection Division of the Department of Justice.</p> | <p>House Bill 116 was signed by the Governor on June 28, 2005. The effective date was not provided in the Bill text or history.</p> <p>The Bill is to be codified at DEL. CODE ANN. tit. 6, §§ 12B-101 through 12B-106.</p> |
| Florida | X | | <p>Any person (conducting business in the state) that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. An</p> | <p>H.B. 481 was approved by the Governor on June 14, 2005, and became effective July 1,</p> |

| State | Statute Enacted | | Summary | Notes |
|---------|-----------------|----|---|--|
| | Yes | No | | |
| | | | <p>administrative fine not to exceed \$500,000 per breach may be levied against any person who fails to give notice within 45 days of (1) a determination of a breach of security; or (2) receipt of notice from law enforcement that notification will not compromise an investigation. Any person who maintains such data on behalf of another business entity must disclose to the business entity any breach of security as soon as practicable, but no later than 10 days following the determination of a breach of security. Any person who fails to disclose within 10 days is liable for an administrative fine not to exceed \$500,000 per breach. Subject to a limited exception, the provisions for administrative sanctions are not applicable to a governmental agency. The procedure and timing for notification is provided by statute. However, the notice requirement is satisfied if subject persons are notified: (1) according to a person or business' own notification procedures, that are consistent with the statute's timing requirements; or (2) according to a security breach procedure pursuant to the guidelines of the primary or functional regulator. If notification of more than 1,000 persons at a single time is required, notice must also be given to all consumer reporting agencies as defined by 15 U.S.C. § 1681a.</p> <p>Notice is not required if after investigation and consultation with relevant agencies, there is no likelihood of harm to customers. The determination must be documented in writing and maintained for 5 years. Failure to do so results in liability for an administrative fine up to \$50,000. Subject to a limited exemption, the administrative fine is not applicable to a governmental agency.</p> | <p>2005.</p> <p>The Bill is codified at FLA. STAT. ch. 817.5681.</p> |
| Georgia | X | | <p>Any information broker that maintains computerized data that includes personal information must give notice of any breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, a person or business that maintains such data on behalf of an information broker must notify the information broker.</p> <p>The proper procedure and timing requirement for giving notice is provided by statute. However, an information broker that maintains its own notification procedures, that are consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach. If the breach requires notification of more than 10,000 residents at one time, the information broker must also notify all consumer reporting agencies (as defined by 15 U.S.C. § 1681a) that compile and maintain files on consumers on a nationwide basis.</p> | <p>S.B. 230 was signed by the governor on May 5, 2005, and became effective as of that same date.</p> <p>The Bill is codified at GA. CODE ANN. §§ 10-1-910 through 10-1-912.</p> |
| Hawaii | X | | <p>Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), <i>or</i> any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section [which is the law enforcement exception contained in all data breach notification laws], and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and</p> | <p>S.B. No. 2290 was signed into law by the Governor on May 25, 2006. The law goes into effect on January 1, 2007.</p> |

| State | Statute Enacted | | Summary | Notes |
|----------|-----------------|----|---|--|
| | Yes | No | | |
| | | | <p>confidentiality of the data system.</p> <p>Notice can be provided as written notice, email notice, or telephonic notice. If the cost of providing individual notice would exceed \$100,000 or the number of people who have to be notified would exceed 200,000 then substitute notice—email notice, conspicuous posting on website, and notification to major statewide media—may be employed.</p> <p>This law provides for a private cause of action, and an individual may sue “any business that violates any provision” of this law for an “amount equal to the sum of any actual damages sustained by the injured party as a result of the violation.” The court in any such action <i>may</i> grant reasonable attorneys’ fees to the prevailing party.</p> | |
| Idaho | X | | <p>An agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.</p> <p>"Breach of the security of the system" means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity.</p> <p>Notice means: written notice, telephonic notice, or notice by email. If the cost of providing notice would exceed \$25,000 or if more than 50,000 individuals would have to be notified, then substitute notification—email notification, conspicuous posting on entity’s website, and notice to major statewide media—may be employed.</p> | S.B. 1374 was introduced on February 10, and signed into law on March 30, 2006. The law went into effect on July 1, 2006. |
| Illinois | X | | <p>Any data collector that owns or licenses personal information concerning an Illinois resident must notify the resident of a breach of security of the system. In the event of a breach, a data collector that maintains (but does not own) computerized data that includes personal information must notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The proper procedure and timing requirement for giving notice is provided by statute. However, a data collector that maintains its own notification procedures, that are consistent with the statute’s timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach.</p> | <p>H.B. 1633 was approved by the Governor on June 16, 2005, and becomes effective on January 1, 2006.</p> <p>The statutory codification of Bill does not appear to have been determined.</p> |

| State | Statute Enacted | | Summary | Notes |
|-------|-----------------|----|--|--|
| | Yes | No | | |
| | | | <p>A waiver of the statute's provisions is unenforceable.</p> <p>A violation constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. Proposed Legislation</p> <p>Illinois H.B. 3743 Creates the Security Breach Notification Act. Requires any person or business conducting business in the State to disclose any breach of the security of the system to any person whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Provides a private right of action for a violation of the Act.</p> <p>H.B. 4198 Amends the Personal Information Protection Act. Requires a data collector to disclose to a consumer, at no cost, the personal information obtained resulting in a breach of the security of the system data.</p> <p>S.B. 209 Creates the Personal Information Protection Act. Requires each financial institution to provide an annual disclosure statement to all persons for which the financial institution maintains unencrypted personal information concerning measures the financial institution has taken to prevent (i) a breach of the security system and (ii) any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the financial institution. Requires each financial institution to maintain duplicate records of all computerized data at a back-up site located at least 90 miles from the primary site at which the data is stored. Provides that the effectiveness of the back-up site shall be tested annually and requires the results of that test to be included in the annual disclosure statement.</p> <p>S.B. 1479 Creates the Identity Theft Notification Act. Requires any data collector that owns or uses personal information in any form that includes personal information concerning an Illinois resident, to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data, without regard for whether the data has been accessed by an unauthorized third party for legal or illegal purposes. Provides that notice may be provided in one of the following ways: (1) written notice; (2) electronic notice; or (3) substitute notice if the person or business demonstrates that the cost of providing notice would exceed \$250,000, or the affected class of persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Provides a private right</p> | <p>The Bill is to be known as the "Personal Information Protection Act."</p> |

| State | Statute Enacted | | Summary | Notes |
|---------|-----------------|----|---|----------------------------|
| | Yes | No | | |
| | | | <p>of action for a violation of the Act.</p> <p>S.B. 1798 Creates the Personal Information Protection Act. Requires any person, business, or State agency conducting business in the State, and that owns or licenses computerized data that includes vulnerable personal information, to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any person whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Requires any person, business, or State agency that maintains computerized data that includes vulnerable personal information that the person, business, or State agency does not own, to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the vulnerable personal information was, or is reasonably believed to have been acquired by an unauthorized person. Provides that notice may be provided to a customer in one of the following ways: (1) written notice; or (2) substitute notice if the person or business demonstrates that the cost of providing notice would exceed \$250,000, or the affected class of persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information.</p> <p>S.B. 1899 Creates the Identity Theft Notification Act. Requires any agency, person, or business that conducts business in Illinois and owns or licenses data that includes personal information concerning an Illinois resident to notify the resident that there has been a breach of the security of that data following discovery or notification of the breach. Requires any agency, person, or business that maintains data that includes personal information concerning an Illinois resident and that the agency, person, or business does not own to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person. Provides that notice may be provided in one of the following ways: (1) written notice; (2) electronic notice; or (3) substitute notice if the agency, person, or business demonstrates that the cost of providing notice would exceed \$250,000, or the affected class of persons to be notified exceeds 500,000, or the agency, person, or business does not have sufficient contact information.</p> <p>S.B. 3040 Amends the Personal Information Protection Act. Provides that the notification requirements of the Act apply to breaches of security concerning written data. Provides that any financial institution that has suffered a breach of security concerning personal information shall provide the owner or licensee of the personal information with free credit watch services for one year, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> | |
| Indiana | X | | Subject to certain limitations, a state agency may not disclose an individual's social security number. | S.B. 503 was signed by the |

| State | Statute Enacted | | Summary | Notes |
|----------|-----------------|----|---|--|
| | Yes | No | | |
| | | | Any state agency that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, a state agency that maintains such data must notify the owner or licensee of the information, and affected state residents. The proper procedure and timing requirement for giving notice is provided by statute. If a state agency is required to provide notice to more than 1,000 individuals, the state agency must also notify all consumer reporting agencies as defined in 15 U.S.C. § 1681a. | Governor on April 26, 2005, and became effective, as of July 1, 2005. The Bill is codified at IND. CODE §§ 4-1-10 through 4-1-11. |
| Iowa | | X | If a person that owns or licenses computer data discovers that a security breach has occurred, the person shall immediately notify the customer, subsequent to the following: a. A law enforcement agency has not determined that notice will impede or compromise a criminal investigation. b. The person has taken the necessary steps to determine the scope of the security breach and has determined how to restore the security of the computer data. (Text from S.S.B. 3019.) | Iowa currently has two bills pending (H.F. 2107, S.S.B. 3019). |
| Kansas | X | | “A person that conducts business in this state, . . . that owns or licenses computerized data that includes personal information shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of personal information has occurred or is reasonably likely to occur, the person . . . shall give notice as soon as possible to the affected Kansas resident.” “‘Personal information’ means a consumer’s first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data element are neither encrypted nor redacted: (1) Social Security Number; (2) driver’s license number or state identification card number; or (3) financial account number, or credit card or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer’s financial account.” The statute contains a safe harbor for companies that “maintains its own notification procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of [the statute].” | On April 19, 2006 the Governor signed into law Senate Bill No. 196 |
| Kentucky | | X | Create a new section of KRS Chapter 367 to require an agency or person or business that conducts business in the Commonwealth, and that owns or maintains computerized data that includes personal information, to disclose any breach of the security of the data to any resident of the Commonwealth whose personal information was acquired, or to any owner or licensee whose information was acquired, by an unauthorized person; create a new cause of action exempted from the State Board of Claims' jurisdiction; amend KRS 65.2001 to conform. | H.B. 175 is currently before the House Judiciary Committee. |

| State | Statute Enacted | | Summary | Notes |
|-----------|-----------------|----|--|---|
| | Yes | No | | |
| Louisiana | X | | <p>After discovering a breach of security, the following entities must notify any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person: (1) any person conducting business in the state that owns or licenses computerized data that includes personal information; and (2) any agency that owns or licenses computerized data that includes personal information. In the event of a breach, an agency or person that maintains such data must notify the owner or licensee of the information. Notification is not required, if after reasonable investigation, it is determined that there is no reasonable likelihood of harm to customers.</p> <p>The proper procedure and timing requirement for giving notice is provided by statute. However, an agency or person that maintains its own notification procedures, that are consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach.</p> <p>A person may institute a civil action to recover actual damages from a failure to disclose in a timely manner any breach of security resulting in the disclosure of personal information.</p> <p>A financial institution that is subject to compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the statute.</p> | <p>S.B. 205 was signed by the Governor on July 12, 2005, and becomes effective as of January 1, 2006.</p> <p>The Bill is to be codified at LAW. REV. STAT. ANN. §§ 51:3071 through 51:3077.</p> <p>The Bill is to be known as the "Database Security Breach Notification Law."</p> |
| Maine | X | | <p>Any information broker that maintains computerized data that includes personal information must give notice of a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. If notice is required, the information broker must also notify the appropriate state regulators or the Attorney General. A person that maintains such data, on behalf of an information broker, must notify the information broker of a breach. The proper procedure and timing requirement for giving notice is provided by statute. If an information broker must notify more than 1,000 people at a single time, notice must also be given to all consumer reporting agencies as defined by 15 U.S.C. § 1681a.</p> <p>Enforcement is entrusted to state regulators within the Department of Profession and Financial Regulation, and the Attorney General. An information broker that violates the statute commits a civil violation and is subject to one or more of the following: (A) a fine of not more than \$500 per violation, up to a maximum of \$2,500 for each day in violation; (B) equitable relief; or (C) enjoinder from further violations. There remedies are cumulative to any other remedies provided at law.</p> | <p>L.D. 1671 (H.P. 1180) was signed by the Governor on June 10, 2005, and becomes effective January 31, 2006.</p> <p>The Bill is to be codified at ME. REV. STAT. ANN. tit. 10 §§ 1346 through 1349.</p> <p>The Bill is to be known as "the Notice of Risk to Personal Data Act."</p> |
| Maryland | | X | N/A | <p>Maryland considered 2005 legislation relating to customer records, security procedures, and data breach (S.B. 1002 / H.B. 1588).</p> |

| State | Statute Enacted | | Summary | Notes |
|---------------|-----------------|----|--|--|
| | Yes | No | | |
| Massachusetts | | X | <p>Proposed Legislation</p> <p>H.B. 4775 Relates to the protection of personal information; defines personal data as any information concerning an individual which can be readily associated with a particular individual; defines security breach and defines reasonable measures data receivers should take to protect against a breach of security. Requires due diligence as relates to third parties and notice of breach.</p> | Massachusetts considered 2005 legislation relating to notification of data breach (H.B. 2797; S.B. 184; and S.B. 2058). S.B. 2058 was set for public hearing on June 23, 2005. |
| Michigan | X | | <p>Sec. 12. (1) Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach to each resident of this state who meets 1 or more of the following:</p> <p>(a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person.</p> <p>(b) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.</p> <p>(2) Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach.</p> <p>(4) A person or agency shall provide any notice required under this section without unreasonable delay. A person or agency may delay providing notice without violating this subsection if either of the following is met:</p> <p>(a) A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. However, the agency or person shall provide the notice required under this subsection without unreasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.</p> <p>(b) A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the</p> | Enrolled S.B. 309 was signed into law on 12/30/06 and will go into effect on July 2, 2007 |

| State | Statute Enacted | | Summary | Notes |
|-----------|-----------------|----|---|--|
| | Yes | No | | |
| | | | <p>agency or person shall provide the notice required under this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.</p> <p>As is typical for data breach laws, the notice must be provided in writing, or by email (if certain conditions are met), or telephone (if certain conditions are met). Substitute notice may also be given “if the person or agency demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed \$250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of this state.”</p> <p>(8) Except as provided in this subsection, after a person or agency provides a notice under this section, the person or agency shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the security breach without unreasonable delay. A notification under this subsection shall include the number of notices that the person or agency provided to residents of this state and the timing of those notices. This subsection does not apply if either of the following is met:</p> <p>(a) The person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents of this state.</p> <p>(b) The person or agency is subject to title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809.</p> | |
| Minnesota | X | | <p>Any person or business (conducting business in the state) that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, a person or business that maintains such data must notify the owner or licensee of the information. If notification of more than 500 people at one time is required, notice must also be given, within 48 hours, to all consumer reporting agencies as defined by 15 U.S.C. § 1681a. The proper procedure and timing requirement for giving notice is provided by statute. However, a person or business that maintains its own notification procedures, that are consistent with the statute’s timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach.</p> <p>The statute does not apply to any “financial institutions” as defined by 15 U.S.C. § 6809(3), and to entities subject to the federal privacy and security regulations adopted under the federal Health Insurance Portability and Accountability Act of 1996. A waiver of the statute’s provisions is unenforceable.</p> <p>The Attorney General and individuals injured by a violation may seek enforcement under MINN. STAT. § 8.31.</p> | <p>H.F. 2121 / S.F. 2118 was approved by the Governor on June 2, 2005, and becomes effective as of January 1, 2006.</p> <p>The Bill is to be codified at MINN. STAT § 325E.61.</p> |

| State | Statute Enacted | | Summary | Notes |
|-------------|-----------------|----|---|---|
| | Yes | No | | |
| Mississippi | | X | <p>Proposed legislation S.B. 2089 Creates the Clean Credit and Identity Theft Protection Act.</p> | |
| Missouri | | X | N/A | Missouri considered 2005 legislation relating to security freeze and data breach (S.B. 506). |
| Montana | X | | <p>A business must take all reasonable steps to destroy or arrange for the destruction of a customer's records containing personal information, which are no longer to be retained.</p> <p>Any person or business (conducting business in the state) that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, a person or business that maintains such data must notify the owner or licensee of the information.</p> <p>The proper procedure and timing requirement for giving notice is provided by statute. However, a person or business that maintains its own notification procedures, that are consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach.</p> <p>If a business discloses a security breach to and gives a notice to an individual that suggests the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice.</p> <p>Any violation constitutes an unlawful practice under the Consumer Protection Act (MONT. CODE ANN. § 30-14-103), and is subject to the penalties provided by § 30-14-142. Upon giving notice, the department may also restrain unlawful violations by temporary or permanent injunction, or temporary restraining order.</p> <p>Any licensee or insurance-support organization (conducting business in the state) that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Any person to whom personal information is disclosed in order for the person to perform an insurance function that maintains computerized data must notify the licensee or insurance-support organization of</p> | <p>H.B. 732 was signed by the Governor on April 28, 2005. In relevant part, the Bill became effective as of March 1, 2006.</p> <p>The Bill is to be codified in Title 30, chapter 14; and Title 33, chapter 19, part 3 of the Montana Code.</p> |

| State | Statute Enacted | | Summary | Notes |
|----------|-----------------|----|--|---|
| | Yes | No | | |
| | | | <p>any breach, if personal information was or is reasonably believed to have been acquired by an unauthorized person.</p> <p>Licenses, insurance-support organizations, and any person to whom personal information is disclosed must develop and maintain (1) an information security policy to safeguard personal information; and (2) a security breach notice procedure that provided expedient notice.</p> <p>Proposed legislation S.B. 33 (LC0454) Requires state and local government agencies to develop procedures regarding social security numbers and to provide notification of a computer security breach of a government agency or third party contracting with government.</p> | |
| Nebraska | X | | <p>Adopts the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006; provides that an individual or commercial entity (defined in the bill to include government, governmental subdivision, and agency) that owns or licenses computerized data that includes personal information about Nebraska residents is to give notice to the affected Nebraska following a security breach of the computerized data system if an investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur; and authorizes the Attorney General to issue subpoenas and seek and recover damages for Nebraska residents injured by violations.</p> <p>Notice can be written notice, email notice, or telephonic notice. If the cost of individually notifying affected Nebraska residents would exceed \$75,000 or if 100,000 residents would have to be notified, substitute notification—email notification, conspicuous posting on the entity’s website, and notification to major statewide media—may be employed.</p> | L.B. 876 was signed into law by the Governor on April 10, 2006. |
| Nevada | X | | <p>A business that maintains records containing personal information concerning customers must take reasonable measures to ensure the destruction of records, which are no longer to be retained. A data collector that maintains records that contain personal information of a resident must implement and maintain reasonable security measures to protect from unauthorized access. A data collector that contracts to disclose personal information of a resident must include a provision requiring the implementation of reasonable security measures. The statute’s requirements are satisfied if the data collector is in compliance with state or federal law requiring greater protection.</p> <p>Any data collector that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, a data collector that maintains such data must notify the owner or licensee of the information.</p> <p>The proper procedure and timing requirement for giving notice is provided by statute. However, a data</p> | <p>S.B. 347 was signed by the Governor on June 17, 2005, and becomes effective as of January 1, 2006.</p> <p>The Bill is to be codified as a new chapter in Title 52 of the Nevada Revised Statutes.</p> <p>The Bill also amends Chapter 597 of the Nevada Revised Statutes to prohibit a business in the state from transferring a customer’s personal</p> |

| State | Statute Enacted | | Summary | Notes |
|---------------|-----------------|----|--|---|
| | Yes | No | | |
| | | | <p>collector that maintains its own notification procedures, that are consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach. A data collector that is subject to and complies with the Gramm-Leach-Bliley Act is also deemed to be in compliance with the notice requirement.</p> <p>If a data collector is required to give notice to more than 1,000 people at one time, notice must also be given to any consumer reporting agency as defined in 15 U.S.C. § 1681a.</p> <p>A data collector that provides statutorily required notice may commence an action for damages against a person that unlawfully obtained or benefited from the personal information obtained from the records maintained by the data collector. A data collector that prevails may be awarded damages including, without limitation, the reasonable costs of notice, attorney's fees, and punitive damages. In addition to other penalties provided at law, the court may order a person convicted of unlawfully obtaining or benefiting from personal information obtained from a breach to pay restitution to the data collector. The Attorney General or district attorney may also bring an action to obtain a temporary or permanent injunction against a violation or proposed violation of the statute. Any waiver of the statute's provisions is unenforceable.</p> | <p>information through electronic transmission other than a facsimile to a person outside the secure system of the business unless the business uses encryption. This amendment become effective October 1, 2008.</p> |
| New Hampshire | X | | <p>Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision. [N.B. This law does not appear to be restricted to New Hampshire residents, only to persons—which includes businesses and governmental agencies—doing business in New Hampshire.]</p> <p>Notice may be electronic, telephonic, or written. If the cost of individually notifying affected persons would exceed \$5,000 or if more than a 1,000 persons would have to be notified, substitute notification—email notification, conspicuous notice on website, and notification to major statewide media—may be employed.</p> <p>This law provides for a private cause of action—damages being capped by the actual damages suffered by the affected individual. The prevailing party will be entitled to reasonable attorneys' fees.</p> | <p>H.B. 1660-FN was signed into law on June 2, 2006, and goes into effect on January 1, 2007.</p> |
| New Jersey | X | | <p>Requires any business that conducts business in New Jersey or any public entity that compiles or maintains computerized records that include personal information to disclose any breach of security of those computerized records to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>The substitute also provides that any business or public entity that compiles or maintains computerized records on behalf of another business or public entity shall notify that business or public entity, who</p> | <p>S.B. 2665 was signed into law on September 22, 2005 and went into effect 180 days later.</p> |

| State | Statute Enacted | | Summary | Notes |
|------------|-----------------|----|--|---|
| | Yes | No | | |
| | | | <p>must then notify its New Jersey customers of the breach; however disclosure is not required if the business or public entity establishes that misuse of the information is not reasonably possible, any such determinations to be documented in writing and retained for five years.</p> <p>Furthermore, the disclosure may be delayed if a law enforcement agency determines that notification will impede a criminal investigation. Notice may be written or electronic. If the business demonstrates that the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business does not have sufficient contact information, it may provide substitute notice, which must consist of all of the following: (1) e-mail notice when the business has an e-mail address; (2) conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and (3) notification to major statewide media. However, a business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of the bill, shall be deemed to be in compliance with the notification requirements of this bill if the business notifies subject persons in accordance with its policies in the event of a breach of security of the system.</p> <p>Additionally, the bill requires a business to take all reasonable steps to destroy customer records within its control containing personal information which is no longer to be retained by the business. The customer records shall be destroyed by shredding, erasing, or otherwise modifying the personal information to make them unreadable or undecipherable through any means.</p> <p>Proposed legislation</p> <p>A.B. 259 Requires businesses to disclose any breach of security of computer systems to customers and to destroy certain personal information no longer retained.</p> <p>A.B. 2104 Creates offenses pertaining to unauthorized use of confidential information; makes it a crime to negligently provide confidential information to a third party without first taking reasonable and adequate steps to ensure the person is authorized to request such information.</p> <p>A.R. 190 Memorializes Congress and President to oppose Financial Data Protection Act of 2005.</p> <p>S.R. 51 Memorializes Congress and President to oppose Financial Data Protection Act of 2005.</p> | |
| New Mexico | | X | N/A | No New Mexico data breach legislation was identified. |
| New York | X | | Requires any state agency, individual, or business that owns or licenses a computerized database that | A.B. 4254 was signed into law |

| State | Statute Enacted | | Summary | Notes |
|----------------|-----------------|----|--|--|
| | Yes | No | | |
| | | | includes vulnerable personal information to disclose any breach of security of such system to any resident of the State whose unencrypted personal information may have been acquired by an unauthorized person. Also requires notice to various State agencies including the Attorney General. | on August 10, 2005, and became effective on December 8, 2005. New York currently has a host of pending legislation (A.B. 1525; A.B. 6688; S.B. 2161; S.B. 3000). New York also considered data breach legislation in each of the 2003, 2004, and 2005 sessions. |
| North Carolina | X | | <p>Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.</p> <p>In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.</p> | H.B. 1248/S.B. 1048 was signed into law on September 21, 2005. The data breach notification section of the law became effective December 1, 2005. |
| North Dakota | X | | <p>Any person (conducting business in the state) that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, a person that maintains such data must notify the owner or licensee of the information. The proper procedure and timing requirement for giving notice is provided by statute. However, a person that maintains its own notification procedures, that are consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach. A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is also deemed to be in</p> | <p>S.B. 2251 was signed by the Governor on April 22, 2005, and became effective on June 1, 2005.</p> <p>The Bill is codified at N.D. CENT. CODE §§ 51-30-01 through 51-30-07.</p> |

| State | Statute Enacted | | Summary | Notes |
|--------------|-----------------|----|--|---|
| | Yes | No | | |
| | | | <p>compliance.</p> <p>The Attorney General is granted enforcement powers as provided in chapter 51-15 and may seek all the remedies in chapter 51-15. Accordingly, a violation is deemed to be a violation of chapter 51-15. These remedies, duties, prohibitions and penalties exist in addition to all others provided by the law.</p> | |
| Ohio | X | | <p>Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.</p> <p>The person shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.</p> <p>The attorney general may conduct pursuant to sections 1349.191 and 1349.192 of the Revised Code an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of this section.</p> <p>These same notification requirements also apply to state agencies.</p> | H.B. 104 was signed into law on November 17, 2005, and became effective on February 17, 2006. |
| Oklahoma | X | | <p>Any state agency, board, commission or other unit or subdivision of state government that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of Oklahoma whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection C of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>Notification can be written or by email. An agency may employ substitute notification—email, conspicuous posting on agency's website, and notification to major statewide media—if the cost of individual notification would exceed \$250,000 or more than 500,000 people would have to be notified.</p> | H.B. 2357 was signed into law on June 8, 2006. |
| Oregon | | X | N/A | Oregon considered 2005 data breach legislation (S.B. 626; S.B. 630; and S.B. 1057). |
| Pennsylvania | X | | An entity that maintains, stores, or manages computerized data that includes personal information shall | S.B. 712 was signed into law |

| State | Statute Enacted | | Summary | Notes |
|--------------|-----------------|----|---|---|
| | Yes | No | | |
| | | | <p>provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 5 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay.</p> <p>When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.</p> <p>A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and Consumer Protection Law. The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.</p> | on December 22, 2005 as Act 94. The effective date is 180 after signing. |
| Rhode Island | X | | <p>A business that owns or licenses personal information about state residents must implement and maintain reasonable security procedures to protect against unauthorized access. A business that contracts to disclose personal information about a resident to a nonaffiliated third-party must include a provision requiring the third-party to implement reasonable security procedures. A business must also take all reasonable steps to destroy or arrange for the destruction of customer records, which are no longer to be retained. Each agency must keep an accurate account of every disclosure made. Each agency must maintain the accounting for at least three years after the disclosure, or until the record is destroyed.</p> <p>A provider of health care, health care service plan, or an entity covered by the medical privacy and security rules of the federal Department of Health and Human Services are exempt. A business regulated by state or federal laws providing greater protection is also exempt.</p> <p>Any person or business (conducting business in the state) that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, a person or business that maintains such data must notify the owner or licensee of the information. The proper procedure and timing requirement for giving notice is provided by statute. However, a person or business that maintains its own notification procedures, which are consistent with the statutes' timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach.</p> <p>Rhode Island's statute also contains a provision relating to the disclosure of information, which requires</p> | <p>H.B. 6191 became effective on July 20, 2005 without the Governor's signature. The Bill became effective as of the date of passage.</p> <p>The Bill is codified at R.I. GEN. LAWS §§ 11-49.2-1 through 11-49.2-9.</p> <p>The Bill is to be known as the "Rhode Island Identity Theft Protection Act of 2005."</p> |

| State | Statute Enacted | | Summary | Notes |
|----------------|-----------------|----|--|---|
| | Yes | No | | |
| | | | <p>subject businesses to provide certain information to customers following a request, if the business had disclosed customer personal information to third parties who have used the information for direct marketing purposes.</p> <p>A waiver of the statute's provisions is unenforceable. Any customer injured by a violation may recover damages. For an intentional or reckless violation, a customer may recover a civil penalty not to exceed \$3,000 per violation. For all other violations, the customer may recover a civil penalty of up to \$500 per violation. Unless the violation is intentional or reckless, a business may assert a complete defense by satisfying certain disclosure requirements within 90 days of learning of a failure to provide information. Any business that violates or proposes to violate the statute may be enjoined from doing so. A prevailing plaintiff may recover reasonable attorney's fees and costs. These rights and remedies are in addition to any others available under the law.</p> | |
| South Carolina | | X | <p>H.B. 3035 Enacts the Identity Theft Protection Act; provides for protections in connection with consumer credit-reporting agencies and with the use and communication of a consumer's social security number, imposition of a security freeze on a consumer's credit report and disclosure of unauthorized access; prohibits requiring the use of personal identifying information on a mortgage.</p> <p>S.B. 8 Enacts the Financial Identity Fraud and Identity Theft Protection Act; relates to consumer credit-reporting agencies, social security numbers, security freezes, and disclosure of unauthorized access to personal identifying information; relates to attorney fees, mortgage records, household garbage, and credit or debit card receipts.</p> | South Carolina considered 2005 data breach legislation (S.B. 669). |
| South Dakota | | X | N/A | No South Dakota data breach legislation was identified. |
| Tennessee | X | | <p>Any information holder must disclose any breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. If personal information was, or is reasonably believed to have been, acquired by an unauthorized person, any information holder that maintains computerized data that includes personal information must notify the owner or licensee of the information in the event of a breach. The proper procedure and timing requirement for giving notice is provided by statute. However, an information holder that maintains its own notification procedures, that are consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach. If a person must notify more than 1,000 people at one time, notice must also be given to all consumer reporting agencies and credit bureaus as defined in 15 U.S.C. § 1681a.</p> <p>Any customer of an information holder (that is a person or business entity, but not a state agency) that is injured by a violation may institute a civil action to recover damages. These rights are in addition to any</p> | <p>S.B. 2220 was signed by the Governor on June 18, 2005, and became effective as of July 1, 2005.</p> <p>The Bill is to be codified in Title 47, Chapter 18, Part 21 of the Tennessee Code Annotated</p> |

| State | Statute Enacted | | Summary | Notes |
|-------|-----------------|----|--|---|
| | Yes | No | | |
| | | | <p>other rights and remedies available under the law.</p> <p>Any person subject to the Gramm-Leach-Bliley Act is exempt from compliance with the statute.</p> | |
| Texas | X | | <p>A business must implement and maintain reasonable procedures to protect and safeguard sensitive personal information collected or maintained by the business from unlawful use. A business must destroy or arrange for the destruction of customer records containing sensitive personal information, which is no longer to be retained. However, a financial institution as defined by 15 U.S.C. § 6809 is exempt from compliance.</p> <p>Any person (conducting business in the state) that owns or licenses computerized data that includes personal information must disclose a breach of security to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In the event of a breach, a person that maintains such data must notify the owner or license holder of the information. The proper procedure and timing for notice is provided by statute. However, a person that maintains its own notification procedure, that is consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach. If a person is required to notify more than 10,000 people at one time, notice must also be given to all consumer reporting agencies as defined by 15 U.S.C. § 1681a.</p> <p>A person who violates the statute is liable to the state for a civil penalty of at least \$2,000 but not more than \$50,000 for each violation. The Attorney General may bring a suit to recover the civil penalty. The Attorney General may also bring an action to restrain a violation or proposed violation by obtaining a restraining order or a permanent or temporary injunction. The Attorney General is entitled to recover reasonable expense in obtaining injunction relief, civil penalties, or both. This includes reasonable attorney's fees, court costs, and investigatory costs.</p> | <p>S.B. 122 was signed by the Governor on June 17, 2005 and becomes effective as of September 1, 2005.</p> <p>The Bill is to be codified at Title 4 of the Business & Commerce Code by adding Chapter 48. See TEX. BUS. & COM. CODE ANN. §§ 48.001 through 48.203.</p> <p>The Bill is to be known as the "Identity Theft Enforcement and Protection Act."</p> |
| Utah | X | | <p>"A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.</p> <p>If an investigation . . . reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident." To be codified at Utah Code Ann. 13-42-202]</p> <p>Personal information means a person's first name or first initial and last name, combined with one of: SSN, financial account or credit or debit card number and access code; or driver's license number "when either the name or data element is unencrypted or not protected by another method that renders the data unreadable or unusable."</p> | <p>S.B. 69 was signed into law on March 20, 2006. The law goes into effect on January 1, 2007.</p> |

| State | Statute Enacted | | Summary | Notes |
|------------|-----------------|----|--|--|
| | Yes | No | | |
| | | | Notification can be provided by first-class mail, electronically if that is the primary way of communicating, telephone, or publishing in a newspaper of general circulation. | |
| Vermont | X | | <p>(1) Except as set forth in subsection (d) of this section, any data collector that owns or licenses computerized personal information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. Notice of the breach shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of the law enforcement agency, as provided in subdivision (3) of this subsection, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.</p> <p>(2) Any data collector that maintains or possesses computerized data containing personal information of a consumer that the business does not own or license or any data collector that conducts business in Vermont that maintains or possesses records or data containing personal information that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subdivision (3) of this subsection.</p> <p>Notice may be provided in writing, email (if certain conditions are met), or by telephone (as long as direct telephonic contact is made with each consumer and does not use a prerecorded message). Substitute notice may be given if the cost would exceed \$5,000 or personal notice would have to be given to more than 5,000 consumers.</p> | Act of General Assembly No. 162 added 9 V.S.A. Chapter 62 ("Protection of Personal Information"). The effective date of this chapter is January 1, 2007, except that the section relating specifically to Social Security Numbers will go into effect on July 1, 2007. |
| Virginia | | X | Requires an individual or a commercial entity that conducts business in Virginia and that owns or licenses computerized data that includes personal information to notify a resident of Virginia of any breach of the security of the system immediately following the discovery of a breach in which unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notification must be made in good faith, in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. The bill also contains alternative notification provisions. For a private civil action to recover damages, the award is triple the amount of actual damages plus reasonable attorney fees. The Office of the Attorney General may also bring an action in law or equity to address violations of this section and other appropriate relief. (Official Summary of H.B. 1154.) | Virginia currently has two data breach bills pending (H.B. 1154; H.B. 1508). H.B. 1154 is currently before the House Science and Technology Committee. |
| Washington | X | | After discovering a breach of security, the following entities must disclose the breach to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person: (1) any agency that owns or licenses computerized data that includes personal information; and (2) any person or business (conducting business in the state) that owns or licenses computerized data that includes personal information. In the event of a breach, any agency, person or business that maintains such data must notify the owner or licensee of the information. | <p>S.B. 6043 was signed by the Governor on May 10, 2005, and became effective on July 24, 2005.</p> <p>The Bill adds a new section to</p> |

| State | Statute Enacted | | Summary | Notes |
|---------------|-----------------|----|---|--|
| | Yes | No | | |
| | | | <p>The proper procedure and timing requirement for giving notice is provided by statute. However, any agency, person, or business that maintains its own notification procedures, that are consistent with the statute's timing requirements, is deemed to be in compliance with the notice requirement if subject persons are notified accordingly in the event of a breach.</p> <p>A waiver of the statute's provisions is unenforceable. In addition to other rights and remedies available under the law, any customer injured by a violation may institute a civil action to recover damages. Any business that violates or proposes to violate the statute may be enjoined from doing so.</p> <p>Any agency, person, or business is not required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.</p> | chapter 42.17 of the RCW; and adds a new chapter to Title 19 of the RCW. |
| West Virginia | | X | N/A | West Virginia considered 2006 data breach legislation (H.B. 4551). |
| Wisconsin | X | | <p>"Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: (1) SSN; (2) driver's license number or state identification number; (3) financial account number, including credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (4) DNA profile; (5) unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.</p> <p>The obligation to "make reasonable efforts to notify each subject of the personal information" that "has been acquired by a person whom the entity has not authorized to acquire the personal information," is triggered by: (a) having principal place of business in Wisconsin or maintaining/licensing personal information in Wisconsin; or (b) maintaining personal information about Wisconsin residents. Notice must be provided within 45 days after the entity learns of the acquisition of the personal information, but this timeline is subject to a law enforcement waiver.</p> <p>No notification need be provided if "[t]he acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information."</p> | Senate Bill 164 was signed into law on March 16, 2006 and became 2005 Wisconsin Act 138. |
| Wyoming | | X | <p>S.B. 53 Relates to consumer protection; provides for notice to consumers affected by breaches of consumer information databases as specified; authorizes consumers to prohibit release of information maintained by credit rating agencies as specified; provides definitions; provides exceptions.</p> <p>S.B. 65</p> | |

| State | Statute Enacted | | Summary | Notes |
|-------|-----------------|----|---|-------|
| | Yes | No | | |
| | | | Relates to consumer protection; provides for notice to consumers affected by breaches of consumer information databases, as specified; authorizes consumers to prohibit release of information maintained by credit rating agencies, as specified; provides definitions; provides exceptions. | |

<http://www.ncsl.org/programs/lis/CIP/priv/breach.htm>

As of 4/9/07